Vigilancia tecnológica en CIBERSEGURIDAD

Confianza digital

Boletín No. 5, 00 de mayo de 2024.

La confianza y las nuevas tecnologías

La percepción de riesgos y la necesidad de construir la confianza digital

El análisis integral de la confianza digital: factores instrumentales y relacionales

Regulaciones para fortalecer la confianza

Tecnologías para reforzar la ciberseguridad

Universidad Nacional Autónoma de México

ICAT Instituto de Ciencias Aplicadas y Tecnología

Directorio

Universidad Nacional Autónoma de México

Rector
Dr. Leonardo Lomelí Vanegas

Coordinadora de Investigación Científica
Dra. María Soledad Funes Argüello

Instituto de Ciencias Aplicadas y Tecnología

Directora
Dra. Ma. Herlinda Montiel Sánchez

Coordinador del Grupo de Gestión Estratégica de la Innovación
Dr. José Luis Solleiro Rebolledo

Autor
José Luis Solleiro Rebolledo

Cuidado de la edición
Norma Solís Mérida

Apoyo en el cuidado de la edición
Eréndira Velázquez Campoverde

Diseño Editorial
Mariana Itzel Barajas Tinoco
Mariana García Delgado
María Fernanda Gasca Alcántara

Contacto
boletinciberseguridadicat@gmail.com

Índice

Presentación

En la economía digital, la información fluye a un ritmo sin precedentes y las interacciones entre personas y organizaciones se realizan crecientemente en espacios virtuales, por lo que la confianza se ha convertido en un elemento fundamental. Las tecnologías digitales como las redes sociales, los teléfonos inteligentes, los pagos electrónicos, las criptomonedas y la *blockchain*, y el manejo de grandes volúmenes de datos se han convertido en elementos indispensables de la vida moderna.

A este fenómeno lo acompaña una creciente brecha de confianza entre los ciudadanos individuales, los consumidores, sus gobiernos y las empresas que generan y despliegan las tecnologías digitales. Muchas personas se preguntan: ¿cómo puedo confiar en alguien a quien nunca he visto?, ¿cómo puedo confiar en una empresa que rastrea tus movimientos todos los días?, y ¿cómo puedes confiar en un algoritmo que toma miles de decisiones por segundo de las cuales ni siquiera se tiene conciencia? (WEF, 2022).

Las encuestas sobre confianza revelan que ha habido un alarmante incremento en la desconfianza en las nuevas tecnologías como la inteligencia artificial, así como en diversas instituciones y sus relaciones. Por ejemplo, la encuesta global sobre la percepción de riesgos realizada por el Foro Económico Mundial, revela que, en el corto plazo, el riesgo más importante en la lista de los primeros diez es el de la información falsa o la desinformación; la ciber-inseguridad ocupa el cuarto lugar. Estos riesgos percibidos se mantienen en la lista de los diez más importantes dentro de diez años, con la notable incorporación del riesgo de efectos adversos de las tecnologías ligadas a la inteligencia artificial.

Figura 1. Encuesta global sobre percepción de riesgos 2023

Fuente: adaptada de WEF (2024).

En tal contexto es donde aparece el concepto de confianza digital (*digital trust*), el cual es una forma de conocer el nivel de confianza que una empresa u organización consigue crear, no sólo con sus clientes, sino también con sus socios y trabajadores en el ámbito del trabajo en línea.

De acuerdo con el Foro Económico Mundial (WEF, por sus siglas en inglés) (2022), "la confianza digital representa la expectativa de los individuos de que las tecnologías y servicios digitales, y las organizaciones que los proveen, protegerán los intereses de los grupos involucrados y que defenderán los valores y perspectivas sociales".

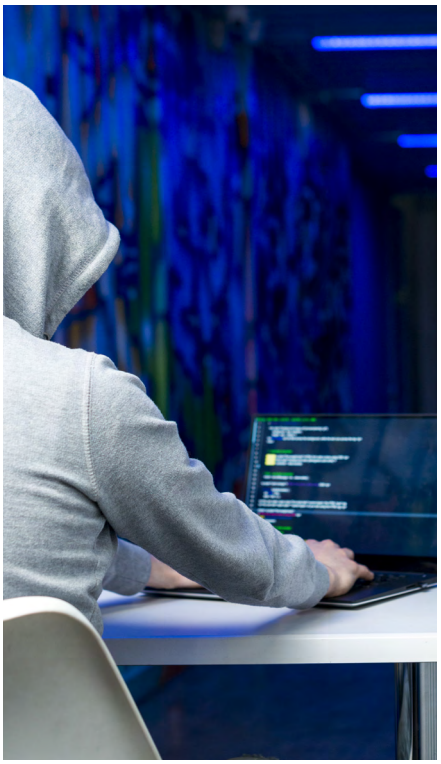
El concepto de confianza digital

La confianza se funda en la certeza de que otros agentes sociales se comportarán de una manera predecible. En la era de la economía digital, el contacto entre clientes y vendedores se realiza crecientemente a través de internet. Por eso se está empleando cada vez más el concepto de confianza digital.

La confianza digital es la expectativa individual de que las tecnologías y servicios digitales, así como las organizaciones que los proveen, protegerán los intereses de todos los involucrados, además de que defenderán sus aspiraciones y valores.

Es claro que la confianza digital, tema central del presente boletín, está muy relacionada con la garantía de que, por un lado, los datos son fiables, de calidad y válidos, además de que el acceso a ellos es legítimo. Sin embargo, se sabe que dichos datos pueden verse comprometidos de diferentes maneras como, por ejemplo, un error humano a la hora de ingresar la información en las bases de datos, un acceso no autorizado o un ciberataque, alterando la integridad de la información o, inclusive, infectando los equipos, lo que puede provocar errores en la transferencia entre dispositivos y daños en los activos digitales.

José Luis Solleiro Rebolledo



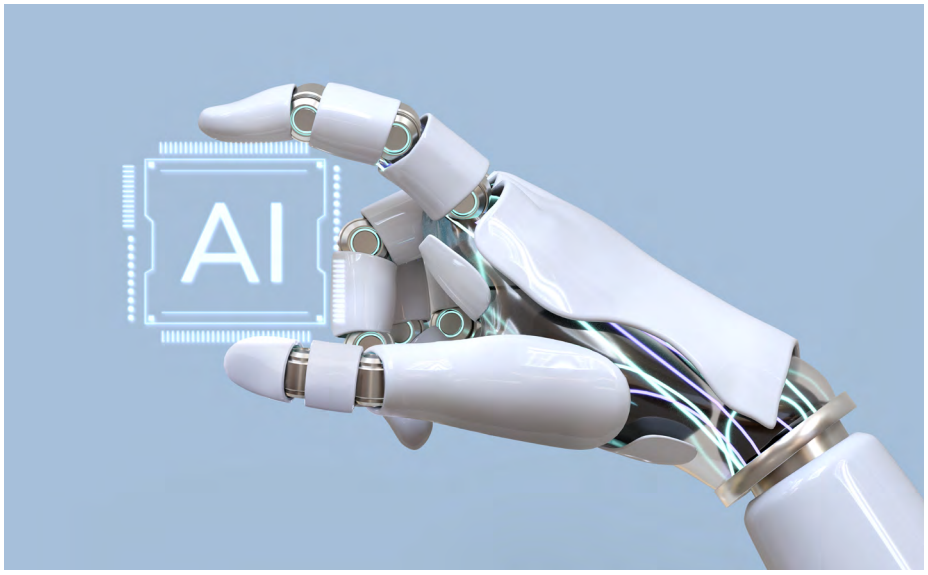
La confianza y las nuevas tecnologías

Los datos y la información son actualmente no sólo un valioso insumo para la producción de bienes y servicios y la toma de decisiones basada en evidencias, sino también un producto que se comercializa en el mercado. En virtud de esta característica de los datos, su gobernanza se ha vuelto un asunto esencial, tanto para los ciudadanos como para las empresas y las administraciones públicas, por lo que se requiere que las instituciones cuenten con estrategias para garantizar la calidad e integridad de los datos para generar y mantener relaciones de confianza.

Actualmente, las nuevas tecnologías conllevan grandes beneficios para la industria, el gobierno y los ciudadanos. En el plano personal, internet ha traído acceso a una gran cantidad de información sobre los más diversos temas; las redes sociales y las aplicaciones de comunicación permiten mantenerse en contacto con amigos y familiares en cualquier parte del mundo; en el entretenimiento, la gran variedad de plataformas digitales ofrece música, películas, series, juegos y materiales educativos; las plataformas de aprendizaje *online*, junto con nuevas estrategias de formación a distancia, facilitan las actividades de educación; mediante el comercio electrónico, hoy se puede adquirir una gran gama de productos y servicios de forma rápida y cómoda.

Para la industria, los beneficios también son considerables. Las nuevas tecnologías digitales permiten trabajar desde cualquier lugar, lo que aumenta la flexibilidad y la productividad, además de reducir costos; las herramientas colaborativas permiten estructurar equipos de trabajo, sin limitaciones de ubicación de sus miembros; la automatización se potencia gracias a los robots y la inteligencia artificial, mediante los cuales se sustituyen tareas repetitivas, de forma que los trabajadores puedan dedicarse a actividades más creativas; mediante el *marketing* digital, las empresas pueden llegar a públicos más amplios, con campañas de promoción basadas en contenidos amplios; y las decisiones empresariales pueden mejorarse gracias a la base analítica que facilita la cantidad de datos disponibles.

Para los gobiernos, la digitalización implica la simplificación de sus actividades, la mejora en la toma de decisiones y tener mayor cercanía con los ciudadanos, mediante plataformas que promueven su participación y la transparencia. Asimismo, las nuevas tecnologías pueden fomentar la inclusión al ofrecer vías efectivas de acceso a la información, los apoyos y las oportunidades emanadas de acciones de gobierno.



La percepción de riesgos y la necesidad de construir la confianza digital

Paradójicamente, los beneficios mencionados vienen acompañados de riesgos pues, a pesar de que la mayoría de la gente reconoce y disfruta esos beneficios, también tiene temores, **fundados o no**, sobre la privacidad, seguridad y potencial uso inadecuado de la información. También existe el temor de que nuestra dependencia de las tecnologías digitales se agudice y que afecte todos los aspectos de nuestra vida (Ramzanovich y Musaevna, 2021).

Concretamente, en lo que concierne a la privacidad y la seguridad de los ciudadanos, se percibe el riesgo de la violación y fuga de datos, el uso inadecuado de herramientas de publicidad dirigida y la posibilidad de que los gobiernos vigilen a las personas mediante el uso de tecnologías de inteligencia artificial. La gente se preocupa crecientemente en torno a cómo se colectan, usan y protegen sus datos. De hecho, el *Barómetro de Edelman,* respecto a la confianza en la tecnología de 2022, concluye que, en promedio, 73% de los que respondieron su encuesta global manifiesta preocupación en cuanto a la privacidad de sus datos (Edelman Trust Barometer, 2022).

La desinformación y la información falsa es otra preocupación que erosiona la confianza de los ciudadanos. Por otro lado, hay grupos de personas que piensan que la inteligencia artificial y la automatización generarán la pérdida de

empleos en diversos sectores y con ello se deteriorará el tejido social. El *Barómetro* 2022 de Edelman concluye que 60% de los encuestados está de acuerdo en que el uso de la tecnología remplazará trabajadores y que esto aumentará la desigualdad.

Finalmente, es importante mencionar que hay temor de que el uso excesivo de redes sociales genere adicción e impactos negativos en la salud emocional y el bienestar de sus usuarios.

Todos estos temores, si bien están más ligados a percepción y no a evidencias concretas, merecen una respuesta concreta y bien planificada para construir confianza digital.

Construyendo la confianza digital

La confianza digital no surge de la nada, sino que se construye a través de la transparencia, la seguridad y la responsabilidad. Las empresas e instituciones que operan en el ámbito digital deben ser transparentes en cuanto al manejo de datos, garantizar la seguridad de la información y actuar de forma responsable, protegiendo los derechos de los usuarios. En el futuro, con el crecimiento de la economía digital, la confianza digital será un requerimiento básico para fortalecer la infraestructura social. Sin duda, se requerirá una combinación de estrategias técnicas, organizacionales y políticas.

En relación con el planteamiento anterior, Chew, Tan y Soon (2023) realizaron una extensa revisión de la literatura internacional sobre el tema de confianza digital, a partir de la cual generan un marco que sirve de referencia para la acción. Los autores referidos destacan la propuesta de Dobrygowsky y Hoffman (2019), quienes dividen el concepto en confianza digital mecánica y confianza digital relacional.

La idea de confianza digital mecánica (o instrumental) se refiere a los mecanismos que entregan resultados predefinidos de manera confiable y predecible. Consideran aplicaciones tecnológicas como la inteligencia artificial, internet de las cosas y *blockchain* como "mecánicas".

Por su parte, la confianza digital relacional es considerada una extensión de la confianza tradicional entre la gente (cuadro 1), analizando cómo influye en la adopción de herramientas digitales. Se ha documentado que la confianza en otra persona o proveedor de servicios digitales determina la decisión de un usuario para utilizar una tecnología.

Cuadro 1. Los factores determinantes en la construcción de confianza digital

Factor para la construcción de confianza digital	Características
Transparencia	Manejar abierta y honestamente la información sobre las acciones y decisiones de una organización, pública o privada, compartiéndola con grupos de interés de forma clara, accesible, completa y oportuna.
Responsabilidad y justicia	Asumir las consecuencias de las acciones y decisiones, con capacidad para responder oportuna y expeditamente ante eventuales fallas o errores. Asumir la responsabilidad de acciones, decisiones, comportamientos y desempeño, ofreciendo información confiable y fidedigna a los grupos de interés. Buscar permanentemente que las reglas y normas se apliquen de forma justa e imparcial.
Equidad y respeto	Tratar a todas las personas de manera justa y equitativa, sin discriminación de ningún tipo. Mostrar siempre consideración por otras personas u organizaciones, atendiendo sus valores, creencias y opiniones. Honrar los compromisos adquiridos y cumplir las expectativas de otras personas y grupos de interés.
Empatía, colaboración y comunicación efectiva	Escuchar activamente, comunicar ideas, situaciones y hechos clara, precisa y oportunamente, poniendo atención en la generación de espacios para el diálogo abierto y honesto.
Marco normativo	La acción de una entidad pública que vele por los intereses y seguridad de los usuarios genera tranquilidad y confianza. Un marco normativo eficaz y actualizado ofrece referencias útiles para ofrecer productos y servicios seguros.
Uso adecuado de tecnologías que mejoren la seguridad de todos los grupos involucrados	La ciberseguridad es un campo cada vez más amplio que involucra una amplia variedad de tecnologías, que son útiles para proteger los equipos informáticos, la información y la integridad de los usuarios. Por eso, el uso de tecnologías y su actualización, genera confianza en el uso de soluciones digitales.

Fuente: elaboración propia.

Se puede observar que, para la construcción de la confianza digital, las personas, las organizaciones y los desarrolladores de políticas necesitan un conjunto de reglas que permitan que sus intereses estén alineados para el uso de la tecnología. De hecho, el Foro Económico Mundial ha lanzado la

propuesta de un marco para ganar confianza digital basado en criterios como la seguridad y confiabilidad, la rendición de cuentas y la supervisión, y el uso inclusivo, ético y responsable, al mismo tiempo que se reconoce la necesidad de ajustarse a las normas de la sociedad en la que opera la tecnología. La figura 2 ilustra el marco propuesto por el Foro Económico Mundial para la construcción de confianza digital.

Figura 2. El marco de confianza digital propuesto por el Foro Económico Mundial

Fuente: adaptada de WEF (2022).

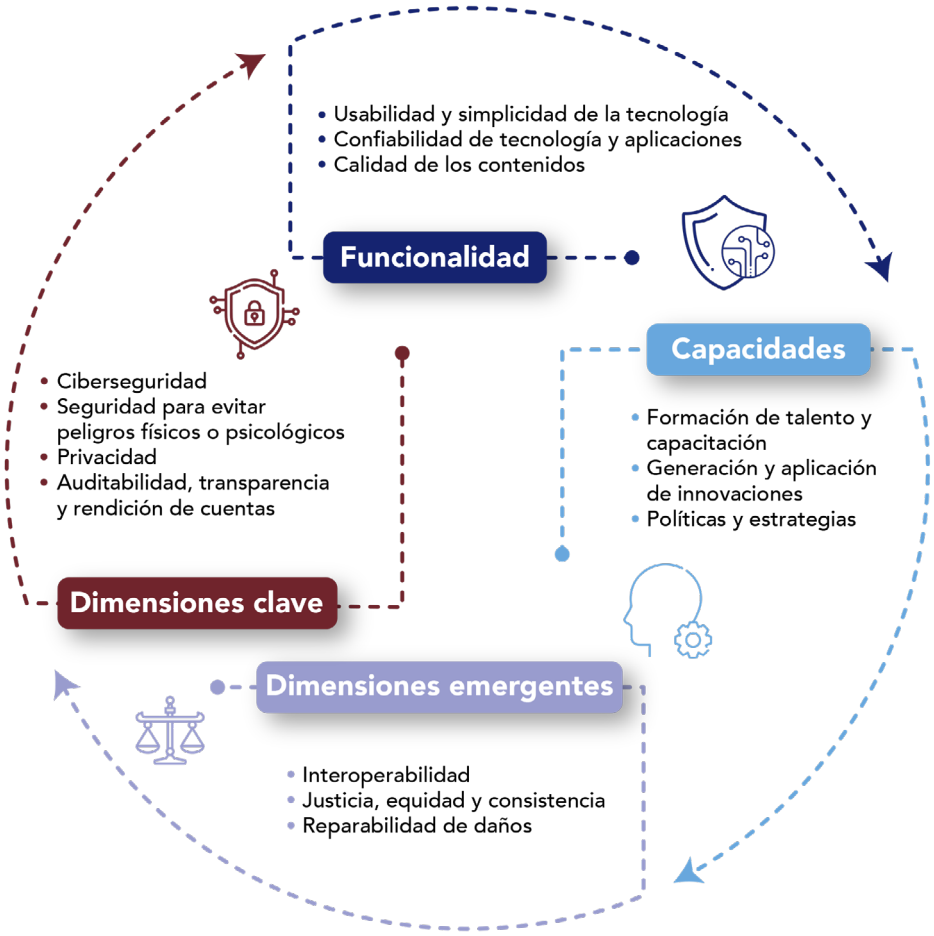
Es claro en esta propuesta que cada criterio da lugar a variables relevantes para el impulso de la confianza digital, las cuales están efectivamente relacionadas con aspectos técnicos y otros relacionados con el enfoque social.

El análisis integral de la confianza digital: factores instrumentales y relacionales

En la construcción de la confianza digital resulta útil desglosar los factores presentados en el cuadro 1 y clasificarlos por su naturaleza instrumental (figura 3) o relacional (figura 4).

La propuesta de Chew, Tan y Soon (2023) para analizar integralmente la confianza digital es muy relevante. Estos autores, basados en su revisión de la literatura, reconocen un enfoque de ecosistema para la construcción de confianza digital que sintetiza los enfoques mecánico y relacional. Bajo tal enfoque, se reconoce que la confianza digital se relaciona con la integridad en las relaciones, interacciones y transacciones entre proveedores y clientes dentro de un ecosistema digital. Este planteamiento indica la importancia de analizar la construcción de la confianza digital a lo largo de una cadena de valor, llevando también a la idea de la responsabilidad compartida. Asimismo, considerando los elementos del marco propuesto por el Foro Económico Mundial, los autores referidos proponen una estructura de los factores mecánicos o instrumentales de la confianza digital que se ilustran en la figura 3. Dichos factores se relacionan con las tecnologías, las capacidades para manejarlas de forma segura y los marcos normativos que regulan su aplicación.

Figura 3. Factores mecánicos o instrumentales para la confianza digital



Fuente: elaboración propia con información de Chew, Tan y Soon (2023).

En cuanto a los factores relacionales, asociados principalmente a las personas para la confianza digital, se reconocen varios relativos a dimensiones interpersonales y otros que destacan las diferencias individuales que llegan a determinar distintas formas de percibir la evolución digital de la sociedad. El tratamiento cuidadoso de estos factores sociales posibilita que se puedan cumplir objetivos de construcción de confianza digital (figura 4).

Figura 4. Factores relacionales de la confianza digital

Fuente: elaboración propia.

El enfoque de ecosistema, los actores y su responsabilidad

Finalmente, en el enfoque de un ecosistema, se reconocen **diversos actores que son parte de la economía digital, cuyas relaciones y su calidad serán determinantes de los resultados en cuanto a la confianza digital**. Los actores más relevantes son:

Usuarios y clientes de servicios digitales

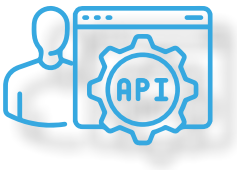
De acuerdo con NINJIO (Cibersecurity Dive, 2024), cerca de tres cuartos de las fugas de datos involucran a personas. Por eso es fundamental la sensibilización y capacitación de los usuarios finales sobre los fundamentos de ciberseguridad, las tácticas usuales de los ciberdelincuentes y las buenas prácticas que debe adoptar un usuario para identificar amenazas y prevenir los ataques. Compartir la responsabilidad contribuirá a generar un entorno más confiable.

Provedores de *hardware* y *software*

Las empresas desarrolladoras de equipo representan la plataforma de innovación que marca en gran medida la trayectoria de la evolución tecnológica. Esto implica una gran responsabilidad en el ecosistema. Por ello, la relación de los proveedores de tecnología y equipo con los operadores y los reguladores es básica para desarrollar conjuntamente un esquema sólido de gobernanza. El modelo de capas de ciberseguridad propuesto por la GSMA (s.f.) es una referencia útil para avanzar en un marco de relaciones constructivas en una cadena de valor segura.

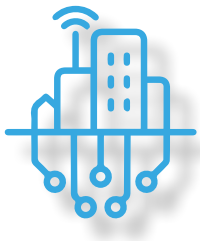
Operadores de servicios de conectividad

Los operadores son el puente que lleva la tecnología a los usuarios, por lo que son pieza clave para construir confianza digital pues son los encargados de desplegar las redes. Su papel es esencial para la construcción conjunta de inteligencia sobre amenazas en tiempo real, un concepto emergente que se enfoca en la detección y mitigación de ciberataques. Compartir información entre los actores del ecosistema evita duplicación de esfuerzos y permite que la detección que efectúa una organización se convierta en medida de prevención para otra (Zrahia, 2018).



Empresas de servicios digitales y desarrollo de aplicaciones

Estas empresas llevan soluciones específicas a los usuarios en diversos sectores, por lo que su apego a las buenas prácticas y su adopción de estándares de ciberseguridad y buen manejo de datos (gobernanza, clasificación, calidad, servicio y agregación de valor a partir de los datos) son factores generadores de confianza digital.



Empresas usuarias de la infraestructura y los servicios digitales

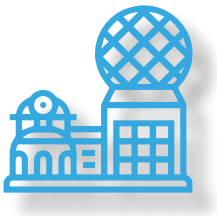
Las empresas que aplican las tecnologías de la información en sus operaciones deben aplicar buenas prácticas y no renunciar a su responsabilidad pensando que la confianza digital la construyen sólo sus proveedores de soluciones. Desde la perspectiva de la ciberseguridad, las cadenas de suministro son tan fuertes como su eslabón más débil, el cual puede ubicarse precisamente en el usuario. Pero se puede mejorar esta situación asegurándose de que cada eslabón (empresa) a lo largo de su cadena de suministro esté protegido contra amenazas cibernéticas.

Entidades gubernamentales

Los gobiernos cumplen una doble función en el ecosistema: son usuarios de soluciones para fortalecer sus capacidades para ofrecer servicios de gobierno electrónico. Por ello, deben adoptar buenas prácticas e interactuar con proveedores de equipo, servicios y soluciones para alinear las estrategias de seguridad. Por otro lado, los gobiernos establecen políticas de desarrollo digital que deberían contemplar medidas de protección y gobernanza de datos, fomento de la innovación, promoción de las relaciones entre los actores del ecosistema y sensibilización de los ciudadanos sobre los beneficios de la economía digital. En la construcción de la confianza digital, los gobiernos tienen mucho por hacer, pues, de acuerdo con el *Barómetro de Edelman* 2023, su credibilidad es la más baja (figura 5).

Reguladores

Las entidades encargadas de la regulación tienen la responsabilidad de desarrollar un marco normativo que genere un entorno seguro para la digitalización de la economía y la sociedad, sin establecer controles excesivos que inhiban la inversión y hagan crecer desmedidamente los costos, al mismo tiempo de que sus decisiones se basan en evidencias y se apegan al principio de neutralidad tecnológica.



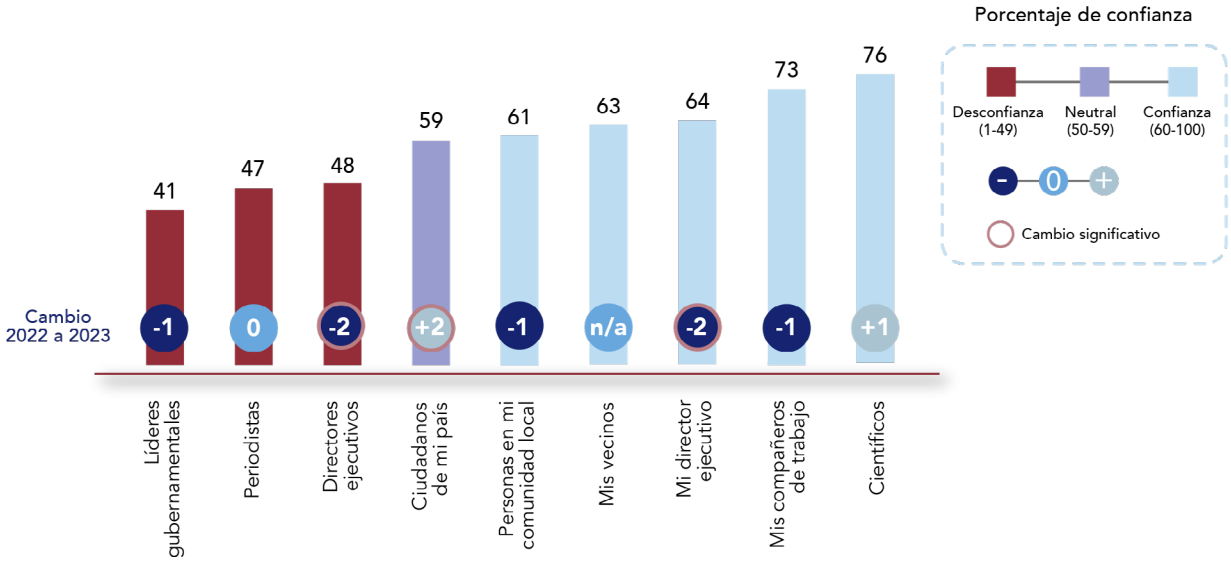
Instituciones de apoyo (universidades y centros de investigación)

La comunidad académica puede jugar un papel muy importante como difusora de información y encargada de sensibilizar a usuarios sobre los pilares de la confianza digital. Como se observa en la figura 5, los científicos son calificados como líderes confiables.

Facilitadores de relaciones en el ecosistema

Hay diversos actores que pueden orientar a los usuarios para que tomen mejores decisiones en su inserción en la economía digital, con mayores niveles de seguridad. Tal es el caso de las instituciones financieras y los inversionistas, que pueden jugar un papel relevante ofreciendo orientación a las empresas sobre la importancia de incluir medidas de ciberseguridad en sus planes de inversión. Otros facilitadores de gran relevancia son los educadores, quienes no deberían mantenerse al margen del fenómeno de cambio que vivimos sino más bien ser parte activa en la sensibilización de las personas sobre los beneficios y las medidas de mitigación de los riesgos.

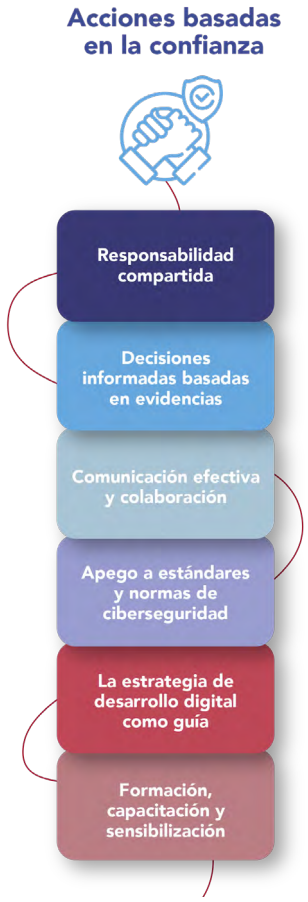
Figura 5. La desconfianza de los líderes institucionales a nivel global



Fuente: adaptada de Edelman Trust Barometer (2023).

Al final, de lo que se trata en este enfoque de ecosistema es de impulsar un esquema de responsabilidad compartida en donde cada uno cumpla con su parte y sea activo en sus relaciones con otros actores. La figura 6 representa una síntesis de las acciones necesarias para construir confianza en la economía digital.

Figura 6. Acciones para construir confianza digital



Fuente: elaboración propia.

Regulaciones para fortalecer la confianza

La creciente cantidad de incidentes y ataques de seguridad relacionados con la información y sistemas informáticos que sufren las organizaciones actualmente ocasiona que sea indiscutible la necesidad de tener controles para garantizar la seguridad de dispositivos, redes de comunicación y activos de información. Por ello, los estándares de ciberseguridad pueden ayudar para contar con una referencia útil sobre buenas prácticas y procedimientos más efectivos.

Las normas y contenidos de los estándares se aprueban por organismos reconocidos a través de comités técnicos que se encargan de definir y justificar especificaciones técnicas que llevan a la ejecución de procedimientos confiables (Taherdoost, 2022). Además, cuando una organización pretende ejecutar un plan de mejora en sus operaciones, la norma le ofrece una línea de base y una referencia para guiar el cambio. Las principales normas internacionales de ciberseguridad son:

ISO/IEC 27000. En realidad, se trata de la familia ISO 27000, que es un conjunto de normas internacionales que proporcionan un marco muy completo para la gestión de la seguridad de la información. La familia incluye las siguientes normas:

- ISO/IEC 27001: Es la norma internacional más reconocida para la gestión de la seguridad de la información. Establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo la gestión de riesgos, controles de seguridad y mejora continua, por lo que es la más importante de la familia y es certificable.

- ISO/IEC 27002: Guía de buenas prácticas para la gestión de la seguridad de la información. Contiene una lista de controles de seguridad que pueden ser implementados por las organizaciones.

- ISO/IEC 27003: Guía para la implementación de la norma ISO/IEC 27001.

- ISO/IEC 27004: Guía para la medición de la seguridad de la información.

- ISO/IEC 27005: Guía para la gestión de riesgos de seguridad de la información.

- ISO/IEC 27006: Guía para la gestión de la seguridad de la información en la cadena de suministro.

- ISO/IEC 27007: Guía para la gestión de la seguridad de la información en las telecomunicaciones.

- ISO/IEC 27017: Guía para la seguridad en la nube.

- ISO/IEC 27018: Guía para la protección de la privacidad.

- ISO/IEC 27031: Guía para la gestión de la seguridad de la información en los servicios de Internet de las Cosas (IoT).

- ISO/IEC 27701: especifica los requisitos y brinda orientación para los organismos que proporcionan servicios de auditoría y certificación de un sistema de gestión de información de privacidad (PIMS) de acuerdo con ISO/IEC 27701 en combinación con ISO/IEC 27001.

- ISO/IEC 27032: Guía para la gestión de la seguridad de la información en los servicios financieros.

- ISO/IEC 27033: Guía para la gestión de la seguridad de la información en los servicios de salud.

- ISO/IEC 27034: Guía para la gestión de la seguridad de la información en el sector público.

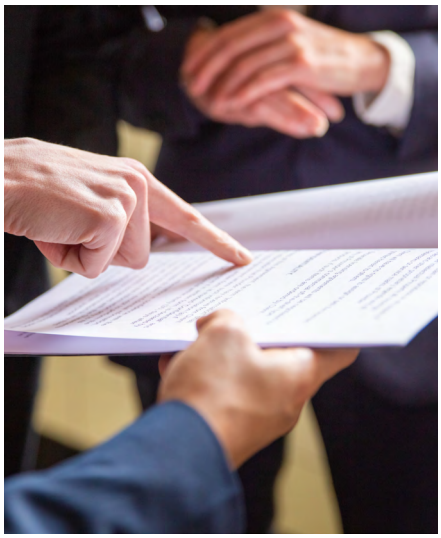
Por su parte, la norma ISO 28000, también conocida como Sistemas de Gestión de la Seguridad para la Cadena de Suministro, es un estándar internacional que ofrece a las organizaciones un marco para identificar, evaluar y controlar los riesgos de seguridad en su cadena de suministro (ISO, s.f.).

Es importante destacar que esta familia de normas, además de cubrir diversos escenarios de ciberseguridad, se mantiene en constante evolución para lograr su alineación con la dinámica de la innovación.

NIST Cybersecurity Framework (CSF). Desarrollado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), el CSF proporciona un marco flexible para la gestión de riesgos de ciberseguridad en cualquier tipo de organización.

SANS Top 25. Este estándar genera una lista de las 25 vulnerabilidades de *software* más comunes que son explotadas por los atacantes. Es una referencia útil para las organizaciones que buscan fortalecer su sistema de protección.

CIS Controls. Desarrollados por el Center for Internet Security (CIS), los *CIS Controls* son un conjunto de 20 medidas de seguridad prácticas y rentables que pueden ayudar a las organizaciones a protegerse de las amenazas cibernéticas más comunes.



GDPR. El Reglamento General de Protección de Datos (GDPR) de la Unión Europea (UE) es una regulación que protege la privacidad y los datos personales de los ciudadanos europeos. Es importante para las organizaciones que operan en la UE o que manejan datos de ciudadanos europeos.

COBIT 5. Es un marco de referencia para el gobierno y la gestión de las tecnologías de la información (TI) en las organizaciones. Incluye principios, políticas y marcos, procesos, estructuras organizativas, información, recursos, servicios y tecnologías, y define 34 objetivos de gobierno y gestión agrupados en cuatro dominios: entregar, asegurar, optimizar y conformar.

NESAS. Esquema de Garantía de la Seguridad de Equipo (GSMA Network Equipment Security Assurance Scheme). La Asociación para el Sistema Global de Comunicación Móvil (GSMA) facilita protocolos y estándares para la tecnología móvil, entre ellos su base de conocimientos para ciberseguridad que es seguida por los principales actores de la industria a nivel global. NESAS aporta un marco para garantizar la seguridad, lo cual eleva la confiabilidad y la confianza en el equipamiento de redes. El objetivo del esquema es auditar y examinar a los proveedores de equipo y sus productos, de acuerdo con una línea de base que constituye el estándar mínimo a cumplir, de tal manera que los operadores de redes móviles puedan verificar la conformidad de los equipos con el estándar deseado.

También se cuenta con un protocolo de pruebas, conocido como Especificaciones de garantía de Seguridad (SCAS, por sus siglas en inglés), mediante las cuales los procesos de desarrollo y gestión del ciclo de vida de productos son auditados, a partir de pruebas de seguridad definidas por el 3GPP (3rd Generation Partnership Project -Proyecto Asociación de Tercera Generación)[1]. Las pruebas relativas

1 Las especificaciones incluyen tecnologías para las comunicaciones por celular (equipo de acceso por señal de radio, capacidades de red y servicio) que aportan una descripción completa de los sistemas para comunicaciones móviles (https://www.3gpp.org/about-us)

a esos requisitos permiten medir objetivamente el nivel de seguridad de los productos de la red. Este esquema ha sido definido por expertos de la industria trabajando con GSMA y la 3GPP, que es una colaboración de grupos de asociaciones de telecomunicaciones, para asentar las especificaciones de un sistema global de comunicaciones de tercera generación.

La mayoría de los proveedores globales de equipo de telecomunicaciones se ha sometido a las auditorías de NESAS y SCAS, con ello aseguran la confiabilidad, la cual se traduce en confianza que se construye sobre hechos verificables.

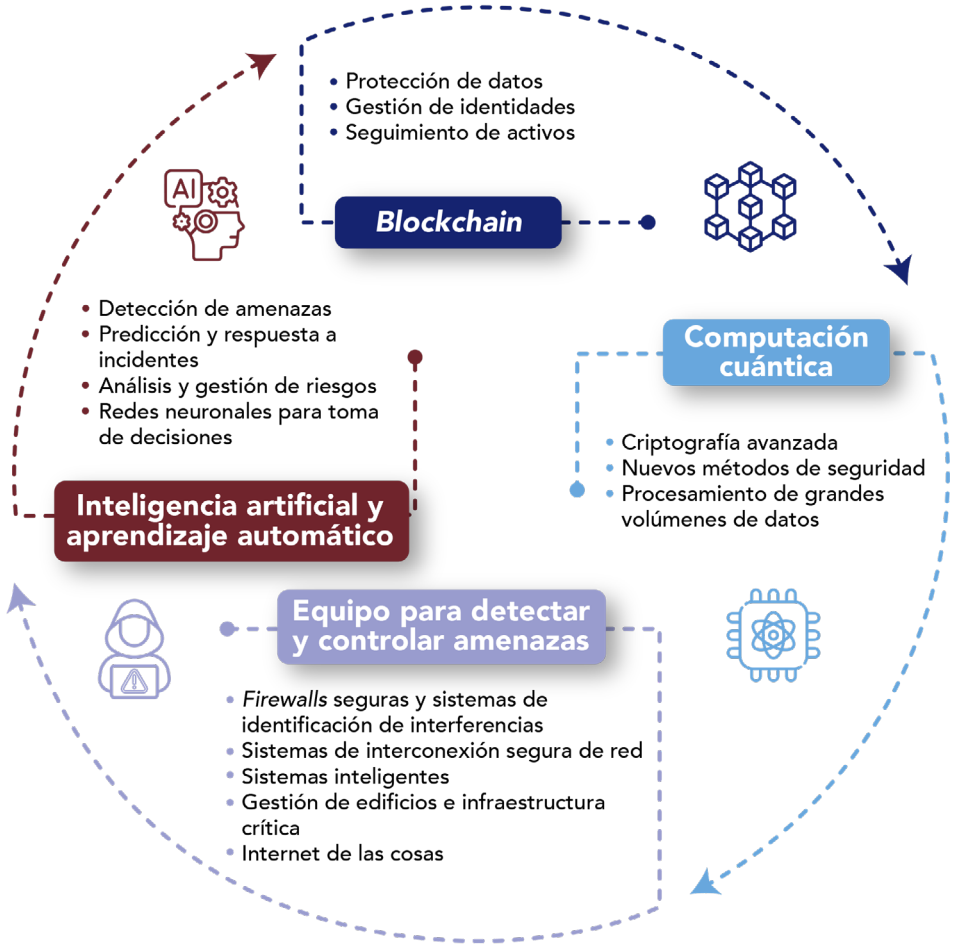
En síntesis, **las regulaciones en materia de ciberseguridad son un instrumento fundamental para proteger a los ciudadanos y las organizaciones en el mundo digital**. A pesar de los desafíos que presentan los posibles ataques, las regulaciones ofrecen beneficios tangibles en términos de seguridad, confianza y desarrollo económico. La cooperación entre gobiernos, empresas y la sociedad civil ha sido clave para asegurar la eficacia de las regulaciones y su evolución de la mano de la innovación, condición que resulta básica para construir un futuro digital más seguro y resiliente.

Tecnologías para reforzar la ciberseguridad

Como las aplicaciones digitales están aumentando y con ello los ataques cibernéticos, la ciberseguridad se está convirtiendo en componente medular de la estrategia de innovación de varias industrias. Desarrollar y aplicar tecnologías eficaces es un elemento central para construir confianza digital. **No es un asunto exclusivo de proveedores de equipo y servicios de ciberseguridad, por lo que el desarrollo de conocimientos en esta área debe ser un esfuerzo colaborativo.** Desarrolladores, fabricantes, operadores y usuarios deben involucrarse en la generación, adaptación y aplicación de soluciones, así como en la formación de capacidades.

Las tendencias tecnológicas para ciberseguridad se concentran en las áreas ilustradas en la Figura 7.

Figura 7. Tecnologías e innovaciones en ciberseguridad



Fuente: elaboración propia.

El análisis de las tendencias tecnológicas (Solleiro, Castañón, Guillén, Hernández, Solís) confirma que la gestión de la ciberseguridad exige inversión en innovación y la coordinación entre muchas entidades públicas y privadas, locales y globales, puesto que se debe buscar proteger infraestructuras, datos, comunicaciones personales de individuos, propiedad intelectual, información de administraciones públicas, procesos y productividad, servicios, *software*, aplicaciones y reputación. Es un asunto verdaderamente esencial para el desarrollo de un ecosistema basado en la confianza.

Reflexiones finales

La confianza digital es la llave que abre las puertas a un futuro digital próspero e inclusivo, pues es un pilar fundamental para el desarrollo armónico de la sociedad en la era digital. Construir y fortalecer la confianza requiere un esfuerzo conjunto por parte de los gobiernos, las empresas, las organizaciones sociales y los usuarios. **Sólo mediante la acción conjunta podremos crear un espacio digital seguro, transparente y responsable que beneficie a todos.**

Los principales pilares de la confianza digital se relacionan con:

- La transparencia que ofrezcan los tomadores de decisiones en los sectores público y privado, pues es muy importante que los usuarios comprendan cómo se recopilan, utilizan y comparten sus datos. Las políticas de privacidad deben ser claras, concisas y accesibles.
- Seguridad en cuanto a la protección de la información personal y financiera, lo cual es vital para la confianza digital. Las medidas de seguridad deben ser robustas y actualizadas para prevenir ataques cibernéticos y fugas de datos.
- Responsabilidad compartida, pues todos los actores del ecosistema de ciberseguridad deben responder por sus acciones y decisiones. Implementar mecanismos de compartición de información, apego a buenas prácticas y desarrollo de un marco para la resolución de conflictos es vital para fortalecer la confianza.

- Ciberseguridad para prevenir y combatir efectivamente los ataques cibernéticos y las fugas de datos que son una amenaza constante que erosiona la confianza. Es necesario invertir en tecnología y estrategias de seguridad para proteger la información.
- Eliminación de la desinformación, ya que la proliferación de noticias falsas y contenido engañoso en internet genera incertidumbre y desconfianza. Es fundamental promover la alfabetización digital y el pensamiento crítico para combatir la desinformación de la sociedad.
- Asegurar la privacidad para atender la creciente preocupación por el uso indebido de datos personales, situación que exige un marco regulatorio sólido que proteja efectivamente la privacidad de los usuarios.

Referencias

3GPP (s.f.). About 3GPP. https://www.3gpp.org/about-us

Chew Han Ei, Tan, J. y Soon, C. (2023). *Digital Trust and Why It Matters.* Institute of Policy Studies, Lee Kuan Yew School of Public Policy, National University of Singapore, Singapore. Recuperado de https://ctic.nus.edu.sg/resources/CTIC-WP-05(2023).pdf

Cibersecurity Dive (marzo de 2024). NINJIO's Latest CISO Report Offers Insights into Growing Role of Cybersecurity in Board Governance. Recuperado de https://www.cybersecuritydive.com/press-release/20240304-ninjios-latest-ciso-report-offers-insights-into-growing-role-of-cybersecur-1/

Dobrygowsky, D. y Hoffman, W. (2019). (28 de mayo de 2019). We Need to Build Up 'Digital Trust' in Tech. *wired.com* Recuperado de https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/

Edelman Trust Barometer (2022). *Special Report: Trust in Technology.* Recuperado de https://www.edelman.com/trust/2022-trust-barometer/special-report-trust-technology

Edelman Trust Barometer (2023). *Global Report*. Recuperado de https://www.edelman.com/sites/g/files/aatuss191/files/2023-03/2023%20Edelman%20Trust%20Barometer%20Global%20Report%20FINAL.pdf

GSMA (s.f.). GSMA Mobile Cybersecurity Knowledge Base. Recuperado de https://www.gsma.com/security/mobile-cybersecurity-knowledge-base/

ISO (s.f.). ISO 9001:2015 - How to use it. Recuperado de https://www.iso.org/publication/PUB100373.html

Ramzanovich, R. y Musaevna, Z. (2021). Digital technologies: problems and trends. *SHS Web of Conferences, 101. 5th International Scientific and Practical Conference 2021 Modern Science: Problems and Development Prospects (Social and Humanitarian Directions).* Recuperado de https://www.shs-conferences.org/articles/shsconf/pdf/2021/12/shsconf_sahd2021_02006.pdf

Solleiro, J. L., Castañón, R., Guillén, A. D., Hernández, T. Y. y Solís, N. (13 de septiembre de 2022*). Vigilancia tecnológica en ciberseguridad. Tendencias tecnológicas*. Boletín No. 2. Recuperado de https://boletinciberseguridadicat.blogspot.com/2022/09/boletin-2-13-de-septeimbre-2022.html

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards-A Review and Comprehensive Overview. *Electronics, 11*(14), 2181-2181. https://doi.org/10.3390/electronics11142181

World Economic Forum [WEF] (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies*. Recuperado de https://initiatives.weforum.org/digital-trust/framework

WEF (2024). *Global Risks Report 2024*. Recuperado de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Zrahia, A. (2018). Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. *Journal of Cybersecurity, 4*(1). Recuperado de https://doi.org/10.1093/cybsec/tyy008

Universidad Nacional Autónoma de México

ICAT
Instituto de Ciencias Aplicadas y Tecnología