Nota: esta traducción está disponible gracias al aporte voluntario de Alejandra Erramuspe. El IGF le está agradecido.

Mensajes IGF 2020

CONFIANZA

¿Qué componentes básicos son esenciales para garantizar una Internet y un mundo en línea que funcione, sea estable y resiliente, que sea lo suficientemente robusto para funcionar en el presente y seguir funcionando bien en el futuro, independientemente del entorno en constante evolución y del panorama de amenazas cambiante?

El COVID-19 dio un vuelco a nuestras vidas y las restricciones para controlar la propagación de la pandemia limitan las actividades cotidianas. Las e-soluciones que nos permiten seguir trabajando o estudiando desde casa, requieren una conectividad segura y estable a una internet confiable. Una internet confiable requiere una infraestructura de internet protegida y fortalecida.

Los países que han establecido un plan de contingencia nacional están mejor posicionados para gestionar las respuestas a desastres de manera más eficaz durante tiempos de crisis. La gestión de estas respuestas debe garantizar la coordinación y alineación en todos los niveles de gobierno, federal, estatal y local, con todos los socios. Esto es importante para desarrollar una respuesta coherente y significativa a las situaciones de emergencia, incluidas aquellas en las que la infraestructura no se ve afectada, como fue el caso de la crisis del COVID-19.

La pandemia COVID-19 es una oportunidad para evaluar e identificar brechas y cuellos de botella en la infraestructura digital, y comenzar a preparar planes de acción para una conectividad asequible y confiable, que asegure suficiente ancho de banda a través de cada tramo de la red y expanda la conectividad a aquellos que aún están desconectados o insuficientemente conectados.

La naturaleza transfronteriza global de internet desafía la noción de soberanía. La colaboración transfronteriza se está convirtiendo en la nueva normalidad. Internet fue diseñada explícitamente para fomentar la interconectividad global, más allá de las fronteras internacionales. Conectar la mayor cantidad posible de personas, dispositivos y redes en una red global de redes, fue y sigue siendo su objetivo central.

Como una medida abrupta e imprevista para luchar contra el COVID-19, gran parte de la población activa se encuentra trabajando desde su casa. Los empleados se conectan a sus redes domésticas en lugar de hacerlo a través de las redes de las empresas bien protegidas, lo que ha aumentado los riesgos ya existentes al tiempo que genera otros nuevos en materia de seguridad. Esta situación

requiere esfuerzos especiales para fortalecer la preparación de la población para enfrentar estos riesgos de seguridad cibernética. El **desarrollo de capacidades, la educación y la formación continua contribuyen a la creación de una cultura de ciberseguridad**.

El rápido crecimiento de los dispositivos domésticos de **IoT** genera preocupaciones sobre las implicancias de seguridad y privacidad para los usuarios. Las directrices, publicaciones y recomendaciones deben publicarse en un formato fácil de usar y utilizando un lenguaje amigable, con menos jerga y terminología técnica.

¿Qué pueden hacer las partes interesadas, desde modelos de gobierno hasta iniciativas concretas para crear una Internet que sea un espacio en línea seguro para todos, respaldado por el respeto de los derechos humanos y la protección de nuestros niños, minimizar los riesgos y daños potenciales a los usuarios? y erradicar la discriminación?

Los gobiernos deben acelerar su transformación digital y desarrollar los canales en línea que son fundamentales para comunicarse y garantizar que los ciudadanos tengan acceso a información importante en tiempos de crisis.

La verificación de hechos (chequeo de información) requiere cooperación local e internacional, y las habilidades y recursos para hacer frente a una avalancha de información, una variedad de fuentes y diversidad de idiomas. Muchas veces, esta verificación, se ve obstaculizada por la presión política y las amenazas financieras y legales.

La verificación de hechos seguirá siendo ineficaz si no se confía en los verificadores de hechos. La participación del gobierno en estas iniciativas, puede fortalecer o socavar esta confianza.

Los bots son herramientas importantes, innovadoras y apropiadas para automatizar tareas en la lucha contra la desinformación. Los recursos ahorrados se pueden concentrar en tareas donde se necesita supervisión humana. La **transparencia** es fundamental para evitar que los bots limiten derechos esenciales, como la libertad de expresión y el acceso a la información. La transparencia tiene muchas capas: el funcionamiento interno de la herramienta, los criterios utilizados y sus efectos, pero también quién está implementando la herramienta y su objetivo.

La producción y difusión de contenido ilegal y nocivo son dos cosas que requieren un alto nivel de vigilancia. La amplificación algorítmica corre el riesgo de automatizar la difusión de lo nocivo.

La educación, la alfabetización mediática y un diálogo público que fomente el respeto por los hechos y la ciencia contribuyen a combatir la desinformación en línea, así como a restaurar la confianza en el periodismo y a una mayor transparencia en la forma en que las empresas de redes sociales (y sus algoritmos) manejan la información. La formación de las habilidades de los jóvenes para el pensamiento crítico debe comenzar desde temprana edad.

Las partes interesadas, los investigadores y los desarrolladores deben asociarse para desarrollar herramientas técnicas y aplicar la inteligencia artificial y el aprendizaje automático, para reconocer y abordar el discurso de odio, la distribución de desinformación y noticias falsas en línea.

El debate y la sensibilización sobre la lucha contra la desinformación y la incitación al odio no pueden posponerse y deben ser fortalecidos. La lucha contra las noticias falsas es una responsabilidad individual y colectiva. Los usuarios deben estar atentos y hacerse responsables de lo que comparten en línea, y no esconderse detrás de la tecnología o transferir toda la responsabilidad a las plataformas de redes sociales.

La tecnología resuelve y crea problemas. El mundo digital está lleno de oportunidades para que los niños aprendan, jueguen, desarrollen su potencial y protejan sus derechos, pero también está lleno de peligros que pueden dañar o socavar sus derechos. Los académicos y especialistas en ciencias del comportamiento y salud mental deben ampliar la investigación sobre el impacto positivo y negativo de las actividades en línea, incluida la influencia de los juegos en el desarrollo y el bienestar de los niños, para que sus hallazgos puedan guiar la formulación de políticas y la práctica de la industria. Los niños, los padres, los educadores, la industria y los legisladores deben participar en el desarrollo de un enfoque equilibrado que gestione los riesgos y maximice las oportunidades.

¿Cómo crear un entorno que fomente un diálogo con las partes interesadas, donde la desconfianza, el miedo y los malentendidos den lugar a la confianza mutua y el reconocimiento del papel de los demás, y todas las partes colaboren en la generación de respuestas integrales a los desafíos de seguridad de nuestro mundo en línea?

Las empresas, el gobierno, la comunidad técnica y las organizaciones multilaterales deben colaborar para desarrollar **respuestas adecuadas** a los desafíos a nivel nacional, internacional y global, derivados de crisis como la del COVID-19.

La pandemia ha demostrado cómo la tecnología y las redes sociales pueden ser un salvavidas para mantenerse en contacto con amigos y familiares, continuar la actividad económica y recopilar información. **El IGF debe facilitar el diálogo sobre la responsabilidad compartida y las acciones de las partes interesadas,** incluida la regulación, cuando sea necesario, para garantizar que los usuarios puedan interactuar y comunicarse en un entorno en línea seguro en todo momento.

Las iniciativas para incluir puntos de vista y perspectivas de múltiples partes interesadas en los diálogos de seguridad cibernética de la ONU son bien recibidas, pero se necesitan más esfuerzos para hacer que los diálogos y las oportunidades de brindar aportes sean más visibles, incluido el apoyo y la creación de capacidades para involucrar a las naciones y comunidades a pesar de la brecha digital. **Las iniciativas de creación de capacidades para los gobiernos de los países en desarrollo deberían prepararlos para participar en las discusiones e iniciativas internacionales y globales sobre cibernormas y reflejar la perspectiva y los intereses de las comunidades locales.**

La protección de los niños y niñas en línea, incluidos los juegos en línea, es un área de políticas emergente y en rápida evolución, y **una parte indispensable de la gobernanza global de Internet**. Todos los interesados deben asumir la responsabilidad, fortalecer la cooperación y coordinar una

combinación adecuada de medidas públicas y privadas, legales y voluntarias, a nivel nacional e internacional. Como práctica estándar, las partes interesadas deben consultar con los niños y niñas sobre asuntos que tienen un impacto en sus vidas, y esto incluye sus vidas en línea.

Las diferencias entre regiones (geográficas, económicas, políticas, culturales) pueden ser significativas y hacer que las mejores prácticas no sean directamente aplicables en todas partes. La participación de múltiples socios es beneficiosa para la creación de capacidades cibernéticas sostenibles. La cooperación y el intercambio de buenas prácticas entre regiones y países con diferente nivel de desarrollo es tan importante como el intercambio entre regiones igualmente desarrolladas. **La confianza entre las partes interesadas intra e interregionalmente fomentará el intercambio de buenas prácticas**. La confianza, la legitimidad y la participación de todas las partes interesadas relevantes son los pilares de cualquier proyecto de creación de capacidad para que resulte beneficioso.

Los **mecanismos de confianza** en el ciberespacio, **basados en principios de responsabilidad, transparencia, respeto, consulta y acuerdo mutuo**, deben establecer **una cooperación abierta entre las múltiples partes interesadas**, incluidos gobiernos, organizaciones internacionales, empresas, comunidades técnicas, instituciones de investigación científica e individuos. Se debe explorar una amplia gama de herramientas como leyes y reglamentos, capacidades de TI, responsabilidad social, ética, supervisión y autodisciplina, así como normas y estándares.

Garantizar la seguridad y la privacidad es esencial para que el ecosistema de IoT prospere, mientras que las pautas y el proceso de toma de decisiones relacionado deben involucrar a diversas partes interesadas, incluida la sociedad civil y los responsables políticos. Hay una falta de conocimiento sobre los riesgos asociados a la implementación de IoT y por ello se hace necesario implementar acciones y desarrollar de capacidades para presentar las mejores prácticas y prevenir amenazas. El IGF se encuentra en una buena posición para colaborar en dicho proceso.