Mitigando riesgos para salvaguardar a México y sus líderes del futuro... ¿Quién nos protege en línea?

Ángel Samuel Reséndiz González
Centro de Estudios Científicos y Tecnológicos "Estanislao Ramírez Ruíz" (CECYT3)
Instituto Politécnico Nacional (IPN)

"No temo a los ordenadores; lo que temo es quedarme sin ellos".
Asimov, I. (s.f.).

Introducción

Vivimos en la era de la información donde la demanda de la tecnología crece y la seguridad informática (ciberseguridad) es una prioridad ineludible para proteger lo que más valoramos: el *conocimiento,* la *educación* y el *liderazgo*. Elementos que aunados impulsarán a los jóvenes para enfrentar desafíos y alcanzar nuestros más anhelados sueños. Isaac Asimov nos recuerda nuestra gran dependencia por la tecnología, que imaginar un mundo sin ella resulta casi imposible.

La tecnología avanza vertiginosamente, pero esta dependencia conlleva riesgos exponenciales. Tan pronto como la humanidad se digitaliza, las innovaciones científicas, tecnológicas y educativas, como la inteligencia artificial (IA), toman un papel cada vez más relevante, convirtiéndose en herramientas promesa, capaces transformar el curso de procesos como la enseñanza y el aprendizaje, pero plantean dilemas éticos como la creatividad humana, lo que requiere de consideraciones diligentes.

En México, donde los futuros líderes crecen inmersos en un mundo digital desde temprana edad, es crucial que, además de ostentar conocimientos y competencias académicas, desarrollen la comprensión profunda e implicaciones de la ciberseguridad. Cultivando una visión a largo plazo que anticipe problemas y aproveche estas tecnologías emergentes para construir un futuro resiliente y prometedor.

Por más que estereotipos sugieren saberes académicos tales como como derivar o integrar (por citar un ejemplo), rara vez tienen aplicación en nuestra vida cotidiana, visto de forma crítica y objetiva podemos apreciar lo contrario. Si los grandes inventores hubiesen adoptado esa visión limitada, podríamos encontrarnos en una era de estancamiento científico y tecnológico, como una tierra reseca que nunca conoció la lluvia de la innovación.

> Por ejemplo, ustedes al leer este ensayo están utilizando dispositivos que incorporan electrónica avanzada, fruto de décadas de evolución tecnológica y si bien, damos por sentados muchos progresos de la humanidad, estos están sumergidos en una ilustración contemporánea y aunque no sean tangibles, representan un hito para las necesidades que afrontamos diario.

En función del desarrollo del siglo XXI, es esencial disponer de una preparación integral capaz de solventar los desafíos técnicos, éticos y sociales derivados de la tecnología y la sociedad. La ciberseguridad no es solo una barrera técnica, sino un pilar que sostiene la resiliencia y, por ende, el futuro que forjamos, garantiza integridad en nuestros entornos digitales y el bienestar de nuestra sociedad en su totalidad.

Proteger adolescentes que usan internet puede ser un tema preocupante puesto que son grupos expuestos. Sabemos que proteger datos y prevenir riesgos digitales garantizará ambientes digitales seguros; por ejemplo, para la educación. Tornándose este tema como componente clave y competitivo para formar líderes y avanzar hacia el sistema educativo. Por tanto, en congruencia, debemos ser conscientes sobre los principales métodos en los ataques cibernéticos e indagar el origen de estos mecanismos para contrarrestarlos y contener una responsabilidad digital acondicionándonos a esta nueva era.

Les exhorto a explorar mediante estas páginas por qué la integración de la tecnología en la educación, el liderazgo, las propuestas para solucionar problemas actuales y muchos otros factores relevantes deben ir complementados de robustas estrategias de seguridad. Proteger para defender el futuro digital de nuestra patria, México.

Desarrollo

Lo abstracto de la seguridad informática y las oportunidades que ofrece

Existe una creencia muy reiterada entre expertos de la informática: ningún sistema es seguro. Esta forma de pensar refleja la realidad técnica de nuestra infraestructura digital y simultáneamente subraya la naturaleza dinámica y compleja del entorno cibernético. Algo válido, históricamente con la aparición de brechas de seguridad que afectaron incluso a las empresas más grandes y tecnológicamente avanzadas de la industria, tal es el caso de la red social Facebook y de Microsoft.

> Por ejemplo, en 2018, Facebook enfrentó uno de sus mayores ataques, dónde más de 50 millones de cuentas de usuarios fueron comprometidas por vulnerabilidades en su código y de manera similar, Microsoft sufrió serios problemas de seguridad, en 2021 se reveló que un grupo de hackers respaldado por el estado chino explotó vulnerabilidades en servidores de correo electrónico *Exchange*, impactando a miles de organizaciones en el mundo. A modo de analogía, estas brechas son apenas una gota en el océano de ciberataques que ocurren diariamente.

Según la revista *"Security Magazine"*, se estima que:

> [...] a nivel mundial, se producen más de 2,200 ciberataques por día, equivalente a un ataque cada 39 segundos. México,

según el periódico *"El financiero"*, se posiciona como el país con mayor número de ataques informáticos a nivel mundial y lo que es más impactante, el Congreso de la Ciudad de México señaló en el 2020 que un gran punto de inflexión de estos ataques y presencia de grupos delictivos en línea surgió durante la crisis sanitaria de la pandemia del *Coronavirus*.

Estadísticas como estás nos recuerdan que la ciberseguridad es una preocupación global que a todos nos concierne. Entonces intervienen dos vertientes, la primera ¿por qué debería preocuparme si no soy un objetivo potencial? Y la segunda, ¿deberíamos de alarmarnos ante esta realidad? Para desglosar ambas vertientes de forma concisa primero se debe entender el vector de ataque frecuente y soluciones que en medida de lo posible debemos implementar tomando un rumbo más allá de los consejos convencionales como el uso de contraseñas fuertes, pues la complejidad del entorno digital exige amplias medidas, posteriormente, reflexionaremos sobre cómo de las adversidades surgen oportunidades, catalizando desafíos para el crecimiento e innovación.

Por último, veremos que la sinergia entre las buenas prácticas de ciberseguridad y el ingenio creativo que caracteriza a los líderes del futuro contribuye a encontrar soluciones factibles para problemas de impacto que someten a nuestra sociedad.

¿Por qué todos somos vulnerables?

Lo digital circunda entre nosotros, niños pequeños pueden usar dispositivos para juegos educativos visto desde un punto de vista pedagógico que les enseñan colores o palabras, mientras que adolescentes y adultos aprovechan la tecnología para su educación, la comunicación, el trabajo o el entretenimiento.

La frase *El ordenador nació para resolver problemas que antes no existían Gates, B. (s.f.)*; fundador de Microsoft, entra en este contexto pues la tecnología incide oportunidades de crecimiento.

Desde los inicios de la informática, las amenazas digitales han cambiado. En el pasado, los *virus troyanos* eran una preocupación significativa; estos programas maliciosos se disfrazaban de programas legítimos para incursionar en los sistemas de las víctimas (Kaspersky, s.f.). Y aunque ya existen mecanismos que detectan y neutralizan amenazas, los ataques también se fortalecieron junto con su sofisticación. Aunque la vulnerabilidad se manifiesta de diferentes maneras como ataques a cuentas bancarias, escolares, incluso las *fake news* que se refieren a noticias falsas, surgen ataques como la ingeniería social considerada como una de las técnicas más peligrosas. Este método manipula a las personas para realizar acciones que comprometan su seguridad.

Por ejemplo, un atacante puede suplantar una figura de confianza, un famoso o un desconocido que solicita ayuda para realizar algo inofensivo, ya sea descargar un programa *(software)*, acceder a enlaces peligrosos, entre otros. La directriz de estos ataques va más allá de un sistema informático, ya que explotan la ausencia de conciencia y la vulnerabilidad inherente en la psicología humana entrando un factor ético, ya que no existe algo símil a un *antivirus* que detecte la mala fe en las personas.

La vulnerabilidad del entorno digital afecta a todas las edades y dispositivos, pero ¿por qué preocuparnos si no somos objetivos puntuales? Reconozcamos que nosotros mismos somos encargados de nuestra seguridad en línea. Solemos subestimar la importancia de nuestra seguridad y más si no somos figuras prominentes, este razonamiento se basa en una inferencia inmediata errónea:

[...] creer que la falta de notoriedad nos excluye de los riesgos, pero tal inferencia representa una falacia lógica, ya que ignora la realidad de los ataques automatizados y masivos que no discriminan por estatus o posiciones sociales.

Si bien, esta perspectiva ignora la complejidad y el alcance de las amenazas actuales, la prioridad en el ciberespacio para explotar vulnerabilidades

comunes radica en la amplia variedad de objetivos medidos por la oportunidad y la susceptibilidad. No ser objetivos concretos, nos hace parte de un fin colectivo dando paso a la recopilación de datos que se convirtió en una industria floreciente para los atacantes en su búsqueda de recolectar información personal y patrones de comportamiento para construir perfiles que, aunque inofensivos al principio, constituyen un impacto significativo como la venta de datos personales.

Otro aspecto es el *efecto dominó*; es decir, la falta de seguridad de un objetivo puede prestarse para atacar a otros a su alrededor, como amigos, familiares y colegas. Un solo acceso comprometido puede expandirse y afectar a más, llevando a consecuencias que van más allá de la víctima inicial. Pese a esto, sucumbir ante el miedo sería errar. La preocupación por nuestra seguridad digital debe traducirse en acción proactiva, *ergo* podemos considerar las siguientes recomendaciones, las cuales trascienden los consejos comunes:

- **Confianza cero *(Zero trust)***
  Esta práctica usualmente es adoptada por empresas y organismos, más podemos aplicarlo tomando una postura de desconfianza hacia cualquier elemento de internet hasta que se confirme su seguridad, veracidad o autenticidad, estableciendo protocolos y barreras que faciliten una respuesta efectiva ante cualquier incidente. Puede lucir excesivo, pero es innegable que la premisa de no confiar sin verificación adecuada resulta altamente eficaz. Un ejemplo de aplicación es para eludir enlaces homógrafos, pues contienen inadvertidas variaciones, donde cambia una "m" por una "n" o una "O" por un "0". Ingresar datos es peligroso pues son detalles casi imperceptibles. Por tanto, tenemos que verificar siempre la autenticidad de todo lo que nos llega o vemos.

- **Diversificación de Contraseñas**
  Usar la misma contraseña en múltiples sitios es una práctica común porque, ¿a quién le gusta recordar contraseñas para todo?, pero puede desencadenar consecuencias ya que, con una sola credencial de acceso filtrada, un atacante podría acceder a más cuentas. La antítesis es considerar el uso de gestores de contraseñas y en conjunto con una autenticación de doble factor añadirá una capa más de seguridad, dificultando así los accesos. Así pues, siempre faltará una segunda verificación ya sea por biométricos o códigos de verificación.

- **Establecimiento de claves de confianza**
  Aquí podemos abatir con la ingeniería social y reforzar el *zero trust* (confianza cero), pues para confirmar identidades entre personas de confianza, podemos implementar una clave de seguridad personal junto con la otra persona, como apodos, lugares o cualquier otro detalle conocido solo por ambos.

- **Precaución con las redes *Wi-Fi* públicas**
  Muchos de nosotros hemos usado redes gratuitas ya sea en centros comerciales, restaurantes e incluso escuelas, pero las redes esconden riesgos que no vemos, como el tráfico de red (nuestros datos enviados y recibidos en una red) y al ser pública no están cifrados, pudiendo ser interceptados por atacantes. Al ingresar a un sitio cualquiera, los datos viajan a manera de solicitudes que pueden ser vistas por el atacante a través del tráfico de red. El riesgo incrementa al introducir contraseñas, enviar mensajes o realizar llamadas. Aunque evidentemente la solución más efectiva sería evitar usar redes públicas, de ser necesario, es recomendable utilizar una red privada virtual (VPN). Ya que cifra el tráfico de red, por lo que cualquier intento de interceptar los datos será evitado.

- **Interacciones con desconocidos en línea**
  Esta práctica no se limita a interacciones directas; esto incluye comentarios en foros o redes sociales. Publicar opiniones controvertidas puede atraer atención no deseada y podría resultar en acoso o ataques en línea. Evitar estos conflictos es una forma de protegernos.

- **Echa un cable a los demás**
  Esta expresión informática hace alusión a ayudar a otros pues el internet no se trata de una cuestión individual, sino colectiva. Apoyar a personas cercanas a protegerse contribuye en una protección adicional. Y como dato, tanto en el campo de finanzas como en la informática, los riesgos nunca se eliminan por completo, solo se mitigan. Y esto nos lleva a hablar de no exponerte más si ya estás en riesgo, al identificar una amenaza, la primera acción deberá ser minimizar tu exposición y contactar a las autoridades para que tomen medidas necesarias. Es mejor buscar apoyo que enfrentar el problema solo.

Incluso cuando existen abundantes técnicas avanzadas de ataques y la presencia de personas malintencionadas, tomar en cuenta medidas oportunas de seguridad como las anteriores, refleja la responsabilidad colectiva y no está alejado de ser un tema interconectado con la ética, la IA y el futuro de México. Los riesgos digitales pueden convertir a un individuo en víctima si no está debidamente informado o prevenido. Abordar aquí estos desafíos de forma razonada, nos proporciona un enfoque preventivo para guiar a los futuros líderes y personas en una navegación segura y ética en el ciberespacio. Pues otra característica que deberán tener los líderes del futuro es saber afrontar desafíos y equilibrar la innovación con responsabilidad ética. La IA y las nuevas tecnologías traerán cambios profundos y opiniones divididas por lo que el papel de los líderes es fundamental para guiar estos avances de forma segura e incluyente.

Bajo análisis y reflexión, ahora examinaremos cómo la ciberseguridad, la IA y la ética están configurando el futuro de la educación y percepciones económicas en México. La IA está transformando no solo la formación de futuros líderes, sino también el marco ético que guiará su toma de decisiones. Para culminar con esta idea, debemos hablar de los *hackers*, término que a menudo lo asociamos con ciberdelincuentes, pero también existe su dialéctico (su opuesto funcional), surgiendo el término de *hacking ético* que se prevé como un campo de crecimiento y percepción económica como oportunidad para enfrentar desafíos actuales.

Impulsado por la demanda para repeler ciberataques, no solo abre nuevas visiones y empleos, sino que también transforma amenazas en ventajas dejándonos clara la capacidad humana e intelectual de convertir la adversidad en una mejora, es válido temer los riesgos asociados con internet, pero el deber y el saber nos exige a actuar de manera mesurada, informada y responsable. Las oportunidades creadas por estos desafíos fortalecen la capacidad de enfrentar los problemas que están por venir.

La dualidad de la educación y la tecnología en México

Sentadas las bases de un entorno digital seguro, reflexionemos cómo este marco impacta en el futuro de la educación, la economía y la formación de líderes en México. La seguridad actúa en consecuencia para que tecnologías emergentes como la IA puedan incorporarse de manera efectiva en el proceso educativo, esto es imprescindible, ya que también actuará como un amplificador de fronteras de la imaginación humana y bajo esta circunstancia, es preciso que los líderes del futuro posean una visión que combine dominio tecnológico con una profunda comprensión ética. Es en la educación donde esta visión debe comenzar a forjarse, al garantizar un medio confiable, creamos un espacio donde se experimente y aprenda sin miedos ni riesgos que afecten perfiles sociales de manera psicológica, por decir un ejemplo.

La educación juega un papel crucial en la ciberseguridad al prevenir que los estudiantes afectados por acoso digital y amenazas opten por la deserción escolar o sufran secuelas psicológicas. Una educación sólida en seguridad digital fomenta su bienestar y éxito académico, las y los jóvenes que enfrentan estos riesgos digitales son los futuros líderes que asumirán roles de liderazgo en México.

El lazo que une tecnología y educación, creará perfiles de profesionales armados de conocimientos avanzados en tecnología y un sólido sentido ético, sirviendo para abordar problemas tan complejos donde podamos agrupar estas ramas interdisciplinarias usando todo lo aprendido y por aprender para cotejar problemas actuales, aprovechando recursos tecnológicos como la IA a favor de cuestiones científicas, humanísticas y de desarrollo valorando las oportunidades que surgen en un entorno económico en constante cambio.

Si la tecnología impulsa la innovación, es esencial gestionar los riesgos asociados; hacerlo no solo protege los avances, sino que también fomenta el progreso científico y social, lo que nos lleva a hablar sobre uno de los retos científicos que afronta México, el desabasto de agua. Enfocar este dilema precisa contar con una perspectiva crítica y objetiva que considere escasez y la contaminación de fuentes hídricas, entonces ¿cómo garantizar esta seguridad hídrica reduciendo simultánea y significativamente el consumo de este recurso?

No solo abarca implementar soluciones existentes como dispositivos ahorradores o sistemas de captación, sino cavilar un enfoque diferenciador de lo descubierto con análisis basado en lo que sabemos y lo que nos falta por descubrir mediante la investigación, principal motor que genera el empuje a las mentes con la chispa del genio creador.

Existen factores importantes que van de la mano de la química, uno de ellos es la fotocatálisis que utiliza luz como fuente para acelerar la descomposición de contaminantes en el agua. Este método, junto con la biorremediación emplea organismos vivos degradando contaminantes, ofreciendo soluciones efectivas para restaurar y asegurar la calidad del agua, aquí, la electroquímica juega un papel fundamental pudiéndose emplear para la desalinización y remoción de metales pesados del agua, también tenemos la ósmosis inversa, que utiliza una membrana semipermeable para separar el agua pura de los solutos, como las sales en aguas marinas. Si se aplica presión al agua salina, sólo las moléculas de agua pasan a través de la membrana, dejando atrás las sales y otros contaminantes, este proceso convierte el agua salada en agua potable, esencial en regiones costeras con escasez de agua dulce. Reducir la contaminación hídrica también contribuye al desabasto, ya que reducirá la necesidad de procesos costosos y energéticamente intensivos de purificación. Disminuirá la carga contaminante, preservará los ecosistemas acuáticos, mejorará la disponibilidad de agua potable y reducirá el consumo significativo en tratamientos adicionales.

Con esto no solo contribuye a la sostenibilidad, sino que también alivia la presión sobre los recursos hídricos, asegurando disponibilidad para próximas generaciones ya que proteger fuentes de agua e implementar tecnologías limpias es esencial para lograr este objetivo cabal. Estos tecnicismos no se alejan de la realidad puesto que, aunque estos procesos no abordan todos los problemas relacionados con el agua, ofrecen salvoconductos para mitigar el problema fuente, abordándolo desde otro punto (la contaminación) y generando conciencia adjunta a la ciencia. Y aunque estas propuestas puedan parecer simples, subestimarlas es errar, esta problemática no puede ser tratada o aislada de la tecnología, ya que son muchas variables las que intervienen en tan complejo problema partiendo desde la falta de consciencia de muchas personas.

Desarrollar y aplicar estos métodos teóricos en laboratorios, contribuirá en avances científicos y tecnológicos siendo la química orgánica, que estudia los compuestos de carbono la que toma presencia en estos estudios, respaldando una vez más el argumento de que los conocimientos

académicos son favorables cuando de solventar problemas se trata, es por esto por lo que esta visión deberá permanecer presente en los líderes que México verá nacer.

Y a todo, ¿cómo se relaciona esto con la ciberseguridad, los desafíos digitales, la inteligencia artificial (IA), la educación y la tecnología? Todo está unido por un punto en común, arraigado en la necesidad de enfoques holísticos y multidisciplinarios para estudiar problemas complejos. Así como problemas actuales requieren un discernimiento profundo de riesgos e implementar estrategias, argumentar propuestas para otras problemáticas ambientales mediante uso de la tecnología demanda soluciones innovadoras y una conciencia sobre su uso eficiente y sostenible. La tecnología y sus emergentes como la ciberseguridad y la IA son nuestra amiga para la revolución 4.0, la educación y más. Dejándonos un valioso aprendizaje. La ciencia y la tecnología comparten un principio esencial:

> [...] la importancia de anticiparse a los problemas y adaptarse a un entorno en constante cambio; contar con la preparación y la conciencia para observar problemas ambientales, tecnológicos, educativos, entre otros, subrayan la necesidad de hacer conciencia ya que transformar el mundo entero es complicado, pero podemos impactar positivamente el mundo de quienes nos rodean dejando una huella politécnica cruzando fronteras del conocimiento.

La orientación de este ensayo es demostrar cómo integrar conocimientos avanzados, buenas prácticas, estándares tecnológicos y ciencia aplicada contribuye a un futuro venidero seguro y sostenible. Juntar innovaciones tecnológicas y educativas nos ilumina un sendero proactivo para entender y enfrentar desafíos globales con soluciones efectivas y adaptables.

Conclusiones

Reflexiones finales, conectando la tecnología con aptitudes, conciencia y con ciencia

En este intrincado universo de desafíos y su inimaginable interconexión con aspectos cruciales de nuestra vida cotidiana, hemos desentrañado problemáticas comunes que nos unen, pues son aspectos relevantes sembrando así, estrategias necesarias. Reconocer hechos, tales como que ningún sistema es completamente infalible o la misma falta de conciencia humana demuestra que la verdadera fortaleza yace en nuestros conocimientos y, como estamos preparados no solo ante la vida, sino ante las oportunidades que se nos presentan siempre con una conciencia moral para salir de apuros globales y personales.

Lejos de inducir miedo a riesgos inherentes que los cambios siempre traen, estas perspectivas nos impulsan a adoptar una templanza resiliente frente a los percances del presente. Fusionar tecnología con habilidades críticas, conciencia moral basada en principios éticos y ciencia, afirmamos que cada desafío siempre trae consigo oportunidades y estas se presentan por todos lados, saberlas identificar y saber hacer algo al respecto es ahora una virtud para los líderes del mañana. Esta perspectiva politécnica fortalecerá varios frentes lo que nos prepara a enfrentar altibajos globales enriqueciendo nuestra visión a futuro. Así, estamos mejor equipados para cimentar un mejor entorno para nuestra nación, donde el conocimiento y la innovación sean pilares de mayores cambios relevantes.

Como politécnicos, llevamos en nuestra sangre los colores guinda y blanco que conforman nuestro ADN con la misión de liderar con innovación y responsabilidad, guiados por el firme propósito de transformar nuestra nación. Este análisis se dispone como una herramienta idónea para dejar una huella perdurable en la historia de México y sus juventudes, haciendo del conocimiento y la creatividad los pilares de un progreso que realmente importe.

Referencias

BBC. (2021). El *inusualmente agresivo* ciberataque del que Microsoft acusa a China (y por qué no es simplemente una nueva crisis de ciberseguridad). Recuperado el 26 de julio de 2024 de: https://www.bbc.com/mundo/noticias-56299627

Congreso de la Ciudad de México (2020). Ciberseguridad. (pp. 01-06). Recuperado el 10 de julio de 2024 de: https://www.congresocdmx.gob.mx/archivos/legislativas/Ciberseguridad.pdf

Calderón, C. (2024) Ciberataques automotrices suben 225% en el país en tres años. Recuperado el 10 de julio de 2024, de: https://www.elfinanciero.com.mx/empresas/2024/05/24/ciberataques-automotrices-suben-225-en-el-pais-en-tres-anos/

Fernández, N. (2015). Manual de laboratorio de Fisiología (pp. 30-34). Nueva York: McGraw Hill Medicina.

Kaspersky. (s.f.) Los siete peligros principales que los niños enfrentan en Internet: cómo mantenerlos seguros. Recuperado el 8 de julio de 2024 de: https://latam.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online

Martínez J. (2024). Estadísticas de ciberseguridad: pronóstico para el 2024 y panorama del 2023. Recuperado el 12 de julio de 2024 de: https://www.deltaprotect.com/blog/estadisticas-de-ciberseguridad-pronostico-2024

Mellado, J. (1999). Fisicoquímica de aguas. Madrid: Díaz de Santos.

Pandora Tech Blogs. (2019). Bill Gates: de joven freak a emprendedor y filántropo forrado. Recuperado el 9 de agosto de 2024 de: https://pandorafms.com/blog/es/bill-gates

Rosen, G. (2018). Actualización de seguridad. Recuperado el 10 de agosto de 2024, de https://about.fb.com/news/2018/09/security-update/

Security Magazine. (s.f.). Los hackers atacan cada 39 segundos. Recuperado el 8 de agosto de 2024 de: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds