

Retos del sector público ante los riesgos de la transformación digital en el contexto de COVID-19

- La pandemia del COVID-19 ha impulsado la transformación digital y con esto también surgen con mayor fuerza riesgos a nivel institucional y del sector público.
- La pandemia del COVID-19 ha impulsado la transformación digital y con esto también surgen con mayor fuerza riesgos a nivel institucional y del sector público.
- Los retos derivados requieren de acciones articuladas en el marco de procesos de rectoría y regulación efectivos, particularmente, en el sector de ciencia, tecnología y telecomunicaciones.

Relevancia

Parte de los fenómenos que ha generado la emergencia sanitaria ocasionada por el COVID-19 ha sido el impulso de las entidades públicas en su transformación digital¹. No obstante, es importante considerar que ante estos cambios, surgen nuevos riesgos cada vez más complejos que requieren gestionarse para mitigar el posible impacto que puedan tener sobre la Administración Pública y finalmente sobre los servicios que se brindan. Es por esto que bajo una visión integral, resulta fundamental comprender que estos riesgos trascienden a las instituciones, y tienen alcance sistémico, por lo que toman relevancia las acciones dentro del Sector Público que se deriven de los procesos de rectoría y regulación.

La transformación digital continúa ante la pandemia

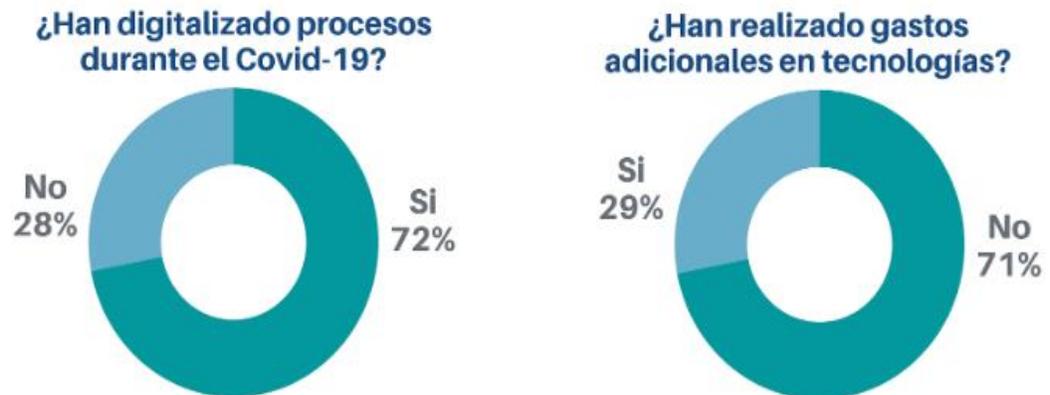
Tal y como se indicó en la reflexión denominada ["El Covid-19 ha acelerado la Transformación Digital en un contexto de brechas institucionales"](#) el COVID-19 ha impulsado la transformación digital en el Sector Público. Al respecto, durante esta pandemia un 72% de las instituciones públicas reportan² modificaciones a algún proceso o procedimiento que antes se ejecutaba de manera presencial o física para que su prestación sea en forma digital. Por su parte, solamente el 29% de las entidades ha requerido realizar gastos adicionales en tecnologías, evidenciando lo señalado en otras ocasiones, en cuanto a que la transformación digital trasciende lo tecnológico (ver gráfico siguiente).

¹ Para más información ver ["El Covid-19 ha acelerado la Transformación Digital en un contexto de brechas institucionales"](#).

² Consulta realizada el 05 de junio de 2020 a 90 entidades públicas que brindan servicios críticos durante la emergencia del COVID-19, de las cuales se contabilizaron 89 respuestas válidas.

Figura N.º 1

Caracterización de la digitalización de procesos del sector público en el Covid-19



Fuente: Elaboración CGR, junio 2020.

Sin duda, la actual pandemia ha implicado ajustes en la forma en que se prestan algunos de los servicios, de modo que muchas entidades han recurrido al uso de herramientas tecnológicas que permitan a la ciudadanía realizar gestiones y recibir los servicios públicos sin la necesidad de desplazarse hacia esas entidades. Estos ajustes conllevan cambios en la interacción con las personas hacia la utilización más intensiva en el uso de plataformas digitales, redes sociales, así como ajustes internos a nivel de procesos y procedimientos.

Ante esta situación, surgen con mayor fuerza riesgos tanto a nivel de cada institución, como del sector público en general, los cuales es pertinente gestionar de forma que se minimicen sus efectos. Esto no solo requiere de medidas que permitan a las entidades públicas adaptarse durante la actual emergencia nacional y se orienten hacia una gestión de riesgos efectiva³, también de acciones articuladas entre actores que permitan lograr mejores resultados de la transformación digital ante la pandemia.

Incremento de riesgos ante la pandemia

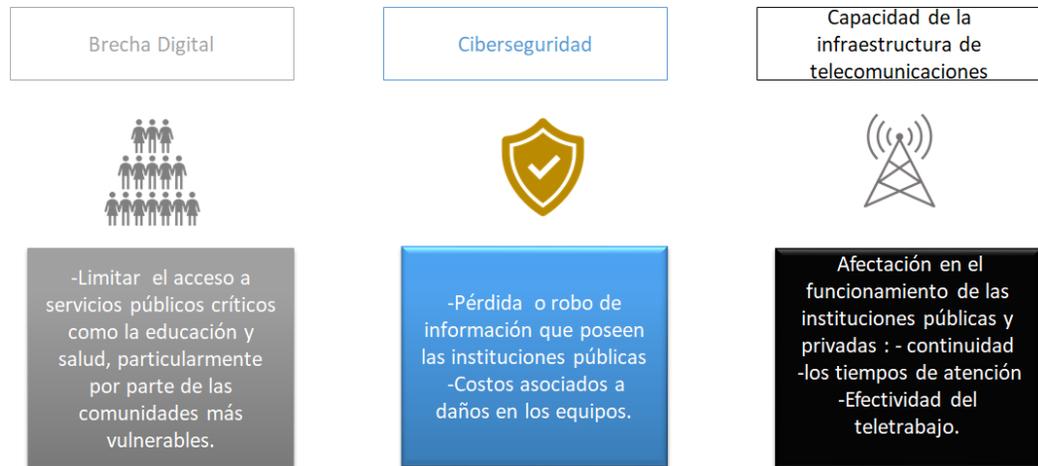
A nivel global, se ha identificado que la pandemia ha incrementado diversos riesgos asociados con la transformación digital⁴ (ver imagen siguiente). Desde una perspectiva agregada sobresalen los riesgos asociados a la brecha digital, la ciberseguridad y a la capacidad de infraestructura de telecomunicaciones,

³ Para más información ver "[El desafío de liderar en tiempos de disrupción: transparencia, eficiencia y sostenibilidad](#)", "[Agilidad y adaptación institucional ante un nuevo paradigma](#)" y "[Decisiones basadas en datos para la gestión del riesgo institucional frente al COVID-19](#)"

⁴ <https://www2.deloitte.com/content/dam/Deloitte/cr/Documents/risk/doc/consideraciones-ciberseguridad-ante-pandemia-global.pdf>

los cuales pueden incidir sobre la continuidad en la prestación de los servicios públicos, así como en la capacidad general del país de enfrentar de forma efectiva la emergencia.

Figura N.º 2
Riesgos asociados en el COVID-19 y la Transformación digital



Fuente: Elaboración CGR, junio 2020.

La brecha digital se refiere a la diferencia entre quienes tienen acceso, de calidad, a las Tecnologías de Información y Comunicación y quienes no lo tienen⁵. Según la última medición del Índice de Brecha Digital, Costa Rica evidencia un nivel medio en el año 2018, manteniendo su calificación respecto del año 2017. Por su parte, el Índice de Progreso Social 2019 del INCAE, muestra la existencia de una brecha a nivel cantonal, específicamente en relación con acceso a información y comunicaciones, en donde el 28% de los cantones mantienen valores inferiores a 70.

Si bien es importante direccionar los esfuerzos del país para que a futuro se reduzcan estas brechas, es posible que los resultados no logren visualizarse en un corto plazo. Aún así, la actual pandemia demanda una respuesta ágil por parte de las entidades y es por esto que un alto porcentaje ha recurrido a una mayor digitalización de procesos, no obstante, resulta fundamental que los cambios que atraviesa el sector público se realicen posicionando a la ciudadanía como eje central para mitigar el impacto que pueda tener la brecha digital sobre el acceso a servicios críticos.

Por otra parte, la ciberseguridad se refiere a la protección de la información que se encuentra, se procesa y se transporta por sistemas de información interconectados⁶. Durante la pandemia se ha identificado un incremento en

⁵ Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2019. *Índice De Brecha Digital*. San José, Costa Rica.

⁶ <https://blog.atlas.com.co/seguridad-informatica-y-seguridad-informacion>

los ciberataques en un 150% a nivel global, particularmente en los sectores de salud, infraestructura y redes móviles⁷ durante los dos primeros meses de la pandemia. En América Latina y el Caribe se registró un aumento de 131% en el mes de marzo en comparación con el mismo periodo del año anterior, en esta línea Costa Rica sufrió aproximadamente a 32 millones de intentos de ciberataques en el primer trimestre del 2020⁸. Se debe tener en cuenta que la ciberseguridad depende no solo de departamentos de tecnologías de información lo suficientemente sólidos, sino también de que las personas encargadas de brindar los servicios públicos tengan una mayor educación sobre los principales riesgos y las formas de prevenir posibles ataques.

Finalmente, la capacidad de la infraestructura de telecomunicaciones se refiere principalmente al medio físico a través del cual fluye el tráfico de internet, incluyendo cables telefónicos, submarinos, satélites, microondas y tecnología móvil⁹. Durante los dos primeros meses de la pandemia, se ha identificado un incremento en el tráfico de datos de al menos un 20% a nivel Mundial, mientras que en Costa Rica durante el primer mes mostró un aumento nacional de al menos un 40%¹⁰, según los reportes de las empresas de Telecomunicaciones. Este incremento implica una mayor exigencia para la infraestructura de telecomunicaciones en cuanto a capacidad y calidad del servicio. De no poder satisfacer esta mayor demanda, el funcionamiento de las instituciones públicas y privadas se podría ver afectado tanto en la continuidad como en los tiempos de atención, así como en la efectividad del teletrabajo.

Retos del Sector Público en el COVID-19 y la Transformación digital

La gestión de los riesgos asociados a la transformación digital requiere de medidas institucionales que permitan asegurar razonablemente la prestación de los servicios públicos de manera inclusiva, segura y continua. Sin embargo, por el potencial impacto de los riesgos asociados a la brecha digital, la ciberseguridad y la capacidad de la infraestructura de telecomunicaciones también se requiere de acciones públicas articuladas en el marco de procesos de rectoría y regulación efectivos, particularmente en el sector de ciencia, tecnología y telecomunicaciones.

A nivel institucional, en entregas anteriores se ha enfatizado la importancia de la gestión de los riesgos institucionales, considerando los diferentes niveles de vulnerabilidad, en procesos operativos, tecnológicos, de recursos humanos y financieros. Como parte de esta gestión de riesgos, también se ha indicado la relevancia de la gestión de la continuidad institucional con medidas que permitan la continuidad de las operaciones y la restauración de los servicios. Todo lo anterior puede ser aplicado para asegurar razonablemente la prestación de servicios públicos de manera inclusiva, segura y continua.

⁷ <http://pubdocs.worldbank.org/en/788991588006445890/Speedboat-Partners-COVID-19-Digital-Development-Joint-Action-Plan.pdf>

⁸ <https://www.fortinetthreatinsiderlat.com/es/Q1-2020/CR/html/trends>

⁹ <https://diag.watch/issues/telecommunications->

[infraestructure#:-:text=Telecommunications%20infraestructure%20is%20very%20similar,generation%20\(5G\)%20mobile%20networks](https://diag.watch/issues/telecommunications-#:-:text=Telecommunications%20infraestructure%20is%20very%20similar,generation%20(5G)%20mobile%20networks)

¹⁰ <https://sutel.go.cr/noticias/comunicados-de-prensa/aumento-en-trafico-de-internet-no-ponen-en-riesgo-el-servicio>

Desde un punto de vista más integral, el sector público también se enfrenta a una serie de retos asociados con la transformación digital en el contexto de la pandemia, siendo que estos se presentan también a nivel global. En este sentido, diversos estudios han identificado desafíos asociados con los riesgos relacionados con la brecha digital, la ciberseguridad y la capacidad de la infraestructura de telecomunicaciones, que se resumen en la siguiente figura (ver imagen siguiente).

Figura N.º 3

Retos del Sector Público en el COVID-19 y la Transformación digital



Fuente: Elaboración CGR, junio 2020.

Como parte de la atención de la brecha digital, se debe promover la inclusividad, que se identifica como el reto de incrementar el esfuerzo de llevar telefonía e internet a las zonas donde se presenta una mayor brecha, bajo la premisa de acceso y servicio universal a poblaciones vulnerables como familias de escasos recursos, personas con discapacidad y adultos mayores. Asimismo, es de vital importancia mejorar las capacidades de ciberseguridad de las instituciones públicas, incluyendo monitoreos constantes, planes nacionales de ciberseguridad, y cooperación público-privada. Finalmente, se encuentra el desafío de anticipar la demanda de servicios de telecomunicaciones y de esta forma prevenir la congestión y saturación del servicio, esto sumado a los de aumentar el ancho de banda, el fortalecimiento de la capacidad de recuperación y de las redes.

Como se observa, las medidas que cada institución pueda ejecutar contribuirán a enfrentar estos desafíos pero serán insuficientes si no responden a acciones articuladas e integrales dentro y entre los diversos sectores. En este contexto, los procesos de rectoría y regulación del sector de ciencia,

tecnología y telecomunicaciones son cruciales para enfrentar los riesgos que se incrementan ante la transformación digital y cuya gestión es crítica para proveer servicios públicos inclusivos, seguros y continuos; muchos de ellos críticos para la ciudadanía en el actual contexto.

Conclusión

La aceleración en el proceso de transformación digital del sector público provocada por la emergencia COVID-19 exige una gestión de riesgos asociados con, la brecha social, la ciberseguridad y la capacidad de la infraestructura de telecomunicaciones del país. Además, ante dichos riesgos, surgen retos que requerirán tanto de medidas institucionales que permitan asegurar razonablemente la prestación de los servicios públicos, como acciones públicas articuladas particularmente en el sector de ciencia, tecnología y telecomunicaciones.

Más información en:

["Riesgos institucionales frente al COVID-19"](#), Contraloría General de la República (2020).

<http://www.oecd.org/sti/ieconomy/recommendation-on-digital-security-of-critical-activities.htm>
