DFOE-FIP-RF-00001-2023
Gestión de la Continuidad: Recuperación de los sistemas que intervienen en el procesamiento de la información para los procesos de ingresos y egresos
Febrero, 2023

Generalidades

Objetivo:

El objetivo de la auditoría es determinar si la gestión de seguridad de la información de los sistemas del Ministerio de Hacienda cumple razonablemente con el marco regulatorio aplicable. Particularmente, el objetivo de este reporte es comunicar condiciones susceptibles de mejora que se identificaron en torno a la continuidad de los sistemas de información.

Alcance y período:

El presente reporte abarca el análisis de la gestión de recuperación de los sistemas que intervienen en el procesamiento de la información para los procesos de ingresos y egresos ante el ciberataque que enfrentó el Ministerio de Hacienda, así como, el impacto para la información presupuestaria del país.

El periodo evaluado comprende desde enero de 2022 hasta noviembre de 2022. Este es el primer reporte de la Auditoría en ejecución; durante el proceso de fiscalización se emitirá también un informe final.

Relevancia:

Al Ministerio de Hacienda como rector del Sistema de Administración Financiera le corresponde la coordinación de las actividades de procesamiento de datos, para procesos como Presupuesto, Tesorería, Crédito Público, Contabilidad, Contratación Pública, recaudación tributaria, gestión aduanera, entre otros. Asimismo, es el responsable de implementar los medios que faciliten el intercambio de datos mediante tecnologías de información y comunicación, con el fin de agilizar los procesos.

Para responder a lo anterior, el Ministerio ha implementado una plataforma tecnológica que permite procesar la información financiera de carácter estratégico, como la liquidación presupuestaria y los Estados Financieros. Además, esta información es base para brindar servicios a la ciudadanía e instituciones públicas.

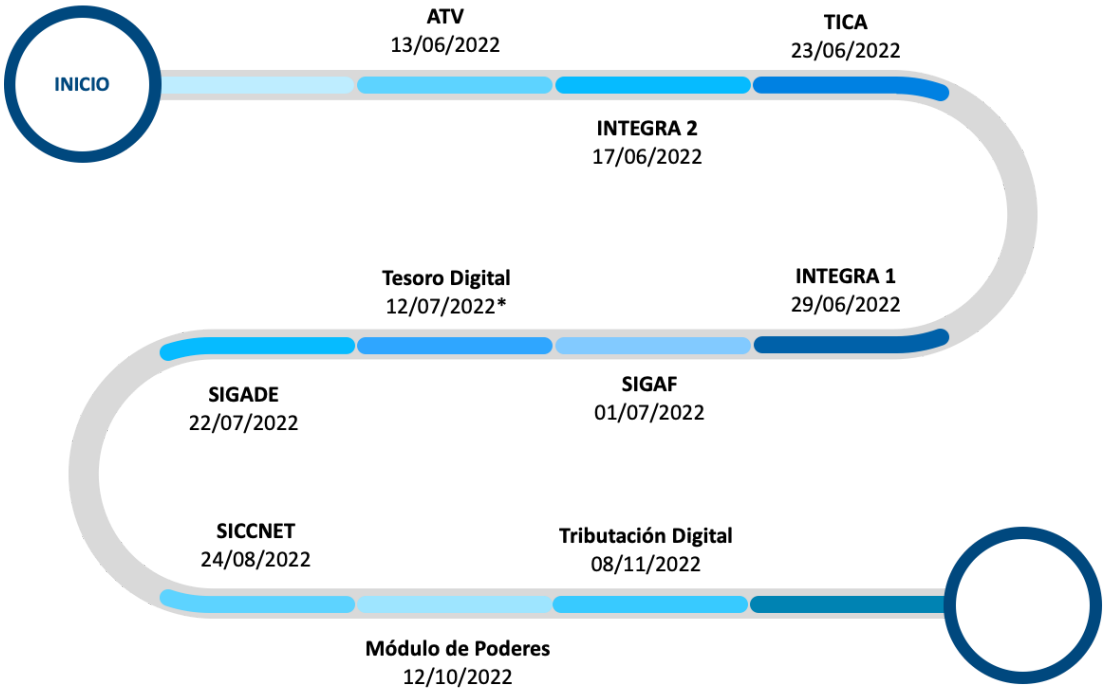
Marco Contextual:

El Ministerio de Hacienda fue objeto de un ciberataque en abril de 2022 ante el cual inhabilitó todos los servicios. Lo que generó la implementación de medidas alternativas para proveer los servicios a la ciudadanía, mientras que el Ministerio evaluaba su plataforma para recuperar la operación normal.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Ahora, el Ministerio paulatinamente ha habilitado los sistemas tras meses de la afectación, lo que implicó la orquestación de diferentes actores para volver a suministrar los servicios a niveles aceptables. La Ilustración N° 1 presenta la fecha de recuperación de sistemas críticos que intervienen en el procesamiento de la información de los procesos de ingresos y egresos.

Ilustración N° 1
Fecha de Recuperación de los Sistemas Críticos que Intervienen en el Procesamiento de la Información de los Procesos de Ingresos y Egreso



Nota: La fecha de recuperación que se indica en la Ilustración es en la que estuvo listo el sistema (ambiente de producción) y con la información al día 18 de abril de 2022.
* La fecha que se consigna corresponde al día siguiente del envío del respaldo al responsable de cargarlo en el sistema Tesoro Digital.
Fuente: Elaboración de la CGR con información de los "Informes de Situación" remitidos por la DTIC.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

La actividad de las organizaciones está sujeta a los principios fundamentales del servicio público para asegurar su continuidad[1]. La continuidad del negocio es la capacidad de una organización para continuar la entrega de productos y servicios dentro de plazos aceptables a una capacidad definida durante un evento disruptivo[2].

Específicamente, la gestión de recuperación es uno de los aspectos abordados por la continuidad de negocio y un elemento del sistema de control interno que permite gestionar la disponibilidad y restablecer procesos o servicios críticos. Su propósito fundamental es desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad y/o servicio[3] que haya sido afectado. Cabe destacar que, la función de "Recuperar" busca la recuperación oportuna para reducir el impacto de un incidente, lo que incluye, la planificación de la recuperación, mejoras y comunicación [4].

Además, la clasificación de procesos o servicios como críticos involucra una determinación de riesgo basada en el impacto derivado del período de tiempo de recuperación. La cual es asignada al realizar el análisis de impacto del negocio y la evaluación del riesgo, y con ello definir el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO). También, algunas organizaciones establecen otros indicadores, como el período máximo tolerable de interrupción (MTPD).

El RPO toma como base la pérdida de datos aceptables e indica el tiempo mínimo posible en el que se pueden recuperar los datos. En tanto que, el RTO es el tiempo improductivo aceptable e indica el punto más próximo en el cual se deben retomar las operaciones. Por su parte, el MTPD es el tiempo en que la viabilidad de la operación sufriría daños irreparables.

Un plan de recuperación tecnológico está integrado por procesos y procedimientos documentados para recuperar y restaurar las actividades del negocio con medidas temporales adoptadas durante y después de una disrupción[5], cuyo objetivo es que la respuesta y el esfuerzo de recuperación sean rápidos, eficientes y efectivos.

---

1 De acuerdo con el artículo 4 de la Ley General de la Administración Pública N° 6227.
2 Punto 3.3 Términos y Definiciones de la Norma INTE/ISO 22301:2020 Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio - Requisitos, segunda edición del 30 de abril de 2020.
3 Por ejemplo: sistemas de información, servidores, bases de datos, aplicativos, comunicaciones, entre otros.
4 Inciso 2.1 del Marco para la mejora de la seguridad cibernética en infraestructuras críticas, Instituto Nacional de Estándares y Tecnología. Versión 1.1 (2018).
5 Punto 8.4.5 Recuperación de la Norma INTE/ISO 22301:2020 Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio - Requisitos, segunda edición del 30 de abril de 2020.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Áreas de mejora identificadas

De acuerdo con la evaluación de las actividades realizadas por el Ministerio de Hacienda para responder y recuperar los servicios, se identificó que se implementaron las recomendaciones emitidas por el MICITT en la Directriz Nº 133-MP-MICITT[6] de acuerdo con las funcionalidades aplicables. También en esa misma línea, la DTIC emitió tres directrices[7] para promover la resiliencia de la infraestructura y la seguridad de la información del Ministerio de Hacienda.

También, implementó medidas de protección como la actualización de privilegios y grupos de la aplicación que almacena y organiza la información sobre los usuarios de red[8]; se aplicó la microsegmentación para mitigar ataques laterales y delimitar mejor el campo de acción de cada uno de los usuarios; hay mejoras de seguridad en la configuración de la VPN; y ahora disponen de medidas preventivas y políticas de seguridad para detectar y abordar eventos de ciberseguridad en tiempo real; entre otras acciones.

Además, se gestionaron recursos de la Comisión de Emergencia para la adquisición de herramientas relacionadas con acciones de recuperación. Por su parte, la Comisión de Coordinación de la Administración Financiera (CCAF) realizó[9] gestiones para solicitar la declaratoria de emergencia informática ante la Presidencia de la República. Y la DTIC definió la creación de un proyecto denominado “Contingencia Tecnológica” que tiene como objetivo estratégico el mantener la operativa de la plataforma tecnológica y de sus sistemas de información.

El Ministerio de Hacienda contó con mecanismos contingentes que le permitieron cumplir con las obligaciones de pago. Al respecto, un mes después ya se habían incorporado 154 instituciones al *Web Banking* y para junio de 2022 ya los Ministerios, con la excepción del TSE y MEP, podían realizar sus pagos por medio de cuentas contingentes habilitadas en Tesoro Digital.

Si bien se realizaron las acciones anteriormente señaladas desde que se presentó el ciberataque en abril del año en curso, esta Contraloría General considera oportuno informar mediante este primer reporte, sobre las áreas de mejora identificadas en relación con la gestión de la recuperación, con el fin de propiciar acciones correctivas que le permitan a la Administración tomar decisiones oportunas en procura de los resultados esperados.

---

6 Directriz “Dirigida a la Administración Pública Central y Descentralizada sobre las mejoras en materia de ciberseguridad para el Sector Público del Estado, del 21 de abril de 2022.

7 Directriz Nº 01-2022 para promover la resiliencia de la infraestructura tecnológica del 06 de mayo de 2022, Directriz Nº 02-2022 para promover la seguridad de la información en la institución del 12 de mayo de 2022 y Directriz Nº 03-2022 para promover la seguridad de la información en el Ministerio del 30 de mayo de 2022.

8 Active Directory.

9 Oficio CCAF 022-2022, del 03 de mayo de 2022.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Oportunidades de mejoras en la planificación de la recuperación posterior al ataque cibernético

La actividad de las instituciones está sujeta a los principios fundamentales del servicio público para asegurar su continuidad[10]. Por su parte, la Política para la Continuidad del Negocio del Ministerio de Hacienda[11] establece que la continuidad de negocio son las acciones preventivas que buscan recuperar y restaurar en el menor tiempo posible, las funciones y procesos críticos. Así como que, se deberá contar con un Plan de Continuidad para todos sus procesos críticos.

Por otra parte, la Política para la Gestión de la Contingencia Tecnológica[12] establece que la Dirección de Tecnologías de Información y Comunicación (DTIC) debe desarrollar, implementar y mantener vigente un plan de contingencia tecnológica de forma que, en caso de un desastre sea posible reanudar las operaciones tecnológicas según los requisitos y prioridades definidas.

Además, las Normas Técnicas para la gestión y control de las Tecnologías de Información del MICITT[13] establece que la institución debe tener prácticas formales que le permitan realizar valoraciones sobre resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones. Así como, que la Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción.

Si bien la planificación de la recuperación no se desarrolló durante y después de la disrupción con base en procedimientos y procesos definidos, lo cual limitó la respuesta rápida, eficiente y efectiva, aún se requiere realizar acciones para finalizar la recuperación posterior al ataque cibernético y estar preparados ante eventuales incidentes.

a) Es importante que el Ministerio defina formalmente el curso de acción para normalizar los servicios a la brevedad posible, dado que, a ocho meses del ciberataque, a pesar de que ya se habilitaron los servicios críticos, no se ha restablecido el 100% de la infraestructura (servidores, bases de datos, aplicativos para monitoreo, entre otros) de los sistemas evaluados[14] y/o hay ajustes pendientes. Al respecto, los encargados funcionales de los sistemas señalaron[15] la existencia de inconsistencias en 55% de los sistemas.

   También, por ejemplo, el Módulo de Poderes y Tributación Digital tiene instaladas versiones de sistemas operativos sin soporte del proveedor. Y en el caso de INTEGRA 2, ePower y Tesoro

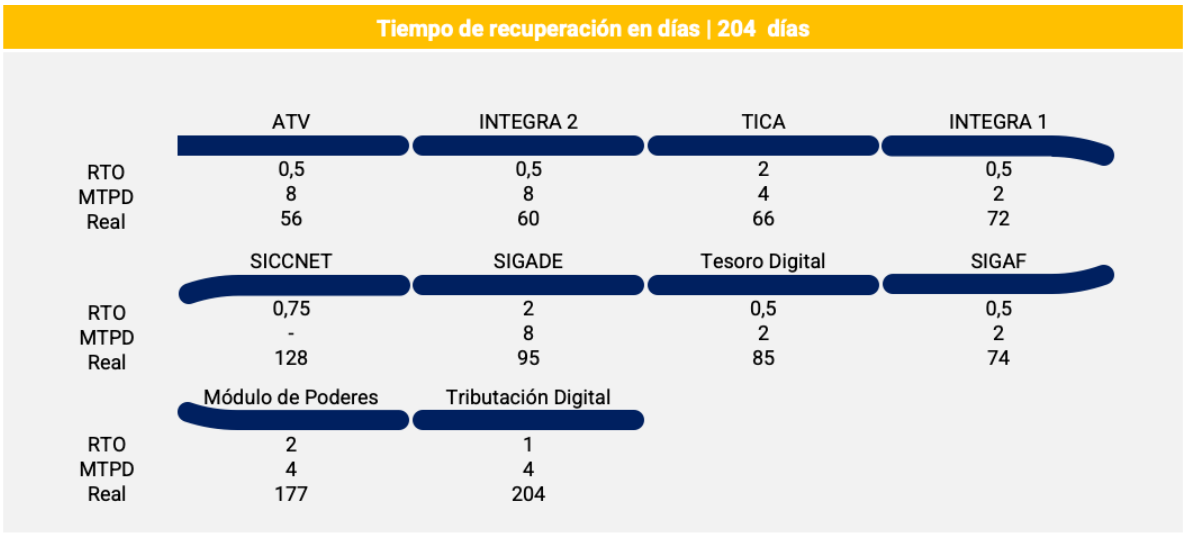
[10] De acuerdo con el artículo 4 de la Ley General de la Administración Pública N° 6227.
[11] Punto 1 y 6.1 de la Política MH-DIPI-PRO02-POL-006 versión 1 de julio de 2019.
[12] Punto 1 de la Política DTIC-POL-036 versión 1 de enero de 2018.
[13] Punto XIII Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos del 10 de noviembre de 2021.
[14] Los sistemas evaluados fueron los siguientes: ATV, INTEGRA 1 y 2, TICA, SIGAF, SIGADE, SICCNET, Tributación Digital, Módulo de Poderes, ePower, SIED y Tesoro Digital.
[15] Información recopilada mediante encuesta realizada a los encargados funcionales.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Digital, el personal de la DTIC indicó desconocer detalles de su operación después del ciberataque dado que está en control de un proveedor.

b) Es importante revisar la resiliencia de la institución y de los sistemas[16] para asegurar la continuidad y hacer frente a un desastre proporcionando un método para restaurar las aplicaciones lo antes posible. Al respecto, los sistemas críticos evaluados[17] se restablecieron en un periodo entre 56 días y 204 días después de su salida de operación (Ver Ilustración N° 2). No obstante, la Administración había definido[18] el punto más próximo en el cual se debió retomar las operaciones (RTO) entre 0,5 y 2 días, así como, el tiempo en que la viabilidad de la operación sufriría daños irreparables (MTPD) entre 2 y 8 días.

Ilustración N° 2
Período Máximo de Interrupción Estimado contra el Período Real



Nomenclatura:
RTO: Objetivo de tiempo de recuperación
MTPD: Período máximo tolerable de interrupción
Real: Tiempo real utilizado por el Ministerio para recuperar los sistemas.

Notas:
1. RTO y MTPD definido por el Ministerio en su análisis de impacto.
2. La cantidad de días real (tiempo de recuperación) que se indica en la Ilustración es en la que estuvo listo el sistema (ambiente de producción) y con la información al día 18 de abril de 2022.

Fuente: Elaboración de la CGR con información suministrada por el Ministerio de Hacienda.

[16] La resiliencia es la capacidad de un sistema de superar una interrupción importante dentro de los tiempos establecidos de recuperación, puede incluir mantener sus capacidades durante la interrupción. ISACA 2019.
[17] Los sistemas evaluados fueron los siguientes: ATV, INTEGRA 1 y 2, TICA, SIGAF, SIGADE, SICCNET, Tributación Digital, Módulo de Poderes, ePower, SIED y Tesoro Digital.
[18] Definido por el Ministerio de Hacienda en su análisis de impacto.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

c) A pesar de que la Política para la Gestión de la Contingencia Tecnológica[19] establece que el equipo asociado al servicio debe realizar los informes sobre las labores de recuperación de los servicios TIC, hay escasa documentación de las labores de recuperación. Lo que implica que el conocimiento obtenido a partir del análisis y la resolución del ciberataque no podría ser utilizado para reducir la posibilidad o el impacto de ataques futuros, así como, restringe la preservación de la información que pueda servir como evidencia de las acciones desarrolladas.

Lo indicado anteriormente, implica habilitar parte de la infraestructura tecnológica pendiente a la brevedad; definir acciones formales que permitan brindar una garantía razonable sobre la continuidad ante nuevas amenazas; así como, documentar las labores de recuperaciones de los servicios de TIC. Ya que, de no lograrse, la institución no podría responder oportunamente ante una eventualidad similar y con ello podría afectar la gestión institucional y demás actores que utilizan los servicios del Ministerio.

Oportunidades de mejora relacionada con la integridad de la información

Las Normas de Control Interno para el Sector Público[20] establecen que la información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defecto, omisiones y modificaciones no autorizadas. Además, debe poseer características que la hagan útil para los distintos usuarios, en términos de pertinencia, relevancia, suficiencia y presentación adecuada, de conformidad con las necesidades específicas de cada destinatario.

Por otra parte, la Política para la Administración de la Infraestructura Tecnológica[21] establece que se debe contar con una estrategia de respaldos y restauración que contenga: la identificación de los datos o sistemas de información por respaldar; la programación por implementar; las acciones de verificación y seguimiento; y los medios idóneos para realizarlos. Además, establece que los medios de respaldo deben contar con la protección ante borrados accidentales, se debe mantener una copia de los respaldos fuera del Centro de Datos; entre otras medidas relativas.

En relación con la información de los sistemas, se requiere la revisión y documentación de la completitud y actualización de la información de los sistemas críticos evaluados[22], que permita brindar una garantía razonable de su integridad, dadas las situaciones que se exponen de seguido:

a) Las dependencias del Ministerio de Hacienda habían[23] definido una pérdida aceptable de datos (RPO) entre 15 y 30 minutos. Sobre lo anterior, la DTIC indicó que recuperó toda la información hasta el último minuto, sin embargo, no se suministró al Órgano Contralor la documentación soporte que permita brindar una garantía de dicha recuperación.

---

19 Punto 1 de la Política DTIC-POL-036 versión 1 de enero de 2018.
20 Puntos 5.61 y 5.6.3 de las N-2-2009-CO-DFOE, versión 2, vigente desde el 6 de febrero de 2009.
21 Punto 6.6.1. Respaldos y Restauración de Sistemas de la Política MH-DTIC-PRO03-POL-001, versión 1 de agosto de 2019.
22 Los sistemas evaluados fueron los siguientes: ATV, INTEGRA 1 y 2, TICA, SIGAF, SIGADE, SICCNET, Tributación Digital, Módulo de Poderes, ePower, SIED y Tesoro Digital.
23 Definido por el Ministerio de Hacienda en su análisis de impacto.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

b) Los encargados funcionales de los sistemas señalaron[24] que verificaron los datos de los sistemas antes de ponerlos en producción en un 64% de los casos. Sin embargo, indican que no disponían de documentación soporte y no comprobaron si la información estaba completa.

c) Once instituciones usuarias de los sistemas de Hacienda afectadas con el ciberataque indicaron[25] que se realizó la carga automática al SIGAF de anticipos, viáticos, transferencias, sentencias, resoluciones y auxilios temporales desde hojas de cálculo, sin embargo, para el resto de información la actualización se realizó mediante procesos manuales, lo que representa riesgos operativos por la cantidad de registros procesados.

   También, cuatro instituciones indicaron conocer de inconsistencias generadas en su mayoría por el procesamiento de información en el sistema INTEGRA. Se mencionan inconsistencias entre las cuales se tienen errores en la relación de puestos vigentes; cargos (movimientos) a las coletillas de suplencias de funcionarios que ya habían sido cesados; problemas con vencimientos de nombramientos; no actualización de las rebajas salariales; errores de lectura de los puestos en caso de ascensos internos y que el sistema no permitió generar el reporte de incentivos.

   Cabe destacar que, seis instituciones señalaron que se dieron errores de pago de salarios y siete instituciones mencionaron conocer de montos a pagar por diferencias salariales. De igual manera, ocho instituciones mencionaron que existen reclamos administrativos por omisión de pagos a proveedores y dos instituciones indican que existieron desembolsos erróneos a proveedores.

   Específicamente en el caso del sistema INTEGRA, la empresa externa que suministra servicios de mantenimiento al Ministerio sobre dicho sistema realizó la carga de las propuestas de pago. Dicha empresa gestionó la verificación de errores en los documentos que los ministerios remitieron, siendo que no se contó con controles adicionales por parte del Ministerio que permitieran corroborar los movimientos realizados. Se está a la espera de que la DTIC finalice la implementación de un proceso automático que permitirá conocer diferencias entre lo pagado y lo que se registró una vez habilitado el sistema.

Además de lo citado anteriormente, el ciberataque afectó la información del sistema de gestión documental que la División de Adeudos Estatales utiliza para almacenar, administrar y controlar el flujo de documentos dentro de la División y el Departamento de Cobro Judicial[26]. Al respecto, se requiere la definición e implementación de las acciones que posibiliten la reconstrucción de la información pérdida. También, la revisión de los acuerdos de respaldo, con el fin de garantizar que toda la información de los sistemas del Ministerio de Hacienda se encuentra respaldada de acuerdo con las necesidades de información. Lo anterior por las situaciones que se comentan a continuación:

---

[24] Información recopilada mediante encuesta realizada a los encargados funcionales que corresponden a, miembros de Comités, personal de las dependencias del Ministerio de Hacienda responsables de los sistemas de información.

[25] Se consultó a once instituciones con el objetivo de conocer los controles implementados durante el período del 18 de abril al 15 de noviembre de 2022, la actualización de la información y la percepción sobre la información brindada por el Ministerio de Hacienda durante el período de contingencia. (Ministerio de Obras Públicas y Transporte; Ministerio de Salud; Ministerio de Hacienda; Ministerio de Seguridad Pública; Poder Judicial; Consejo Nacional de Vialidad; Ministerio de Justicia y Paz; Ministerio de Trabajo y Seguridad Social; Registro Nacional; Dirección Nacional de Centros de Educación y Nutrición y de Centros Infantiles de Atención Integral; y el Ministerio de Educación)

[26] Informe Técnico sobre encriptación de unidad de información no estructurada del sistema ePower, de octubre de 2022.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

a) La información que no se recuperó está relacionada con los procesos de cobro, arreglo de pago, prescripciones, daciones, e incobrabilidad. Esto corresponde a 12.000 solicitudes de prescripción digitalizadas; 25.000 expedientes de cobro digitalizados; 18.023 expedientes de cobro asignados a los fiscales que representan un monto de ¢341.216 millones[27]. Lo citado expone al Ministerio a que venzan los plazos de prescripción de las deudas y se imposibilita poder cumplir con los requerimientos y solicitudes de certificación de expedientes que llevan a cabo los Órganos Contralores y la Procuraduría General de la República.
b) En cuanto al resguardo de información previa al ataque, la DTIC indicó[28] que se omitió en la solicitud de respaldos diarios de la base de datos el repositorio que contenía las imágenes de los expedientes. También, a pesar de que se hacían respaldos de máquinas virtuales mensualmente, no se encontraron respaldos vigentes y operables, dado que habían cumplido su ciclo de retención.

Así las cosas, es necesario documentar la completitud y actualización de la información, así como, tomar las medidas para la restructuración de la información pérdida, que permita la toma de decisiones con base en información de calidad, que propicie la transparencia y la rendición de cuentas.

Oportunidades de mejora en la coordinación y comunicación de las acciones de recuperación con los actores relevantes

De acuerdo con las Normas ISO[29] la organización debe implementar y mantener una estructura de respuesta que permita una alerta oportuna y comunicación relevante a las partes interesadas. Además, establece que se debe documentar y mantener procedimientos para comunicarse interna y externamente, incluyendo qué, cuándo, con quién y cómo comunicarse; asegurar la disponibilidad de los medios de comunicación durante la disrupción; facilitar la comunicación estructurada con el equipo de emergencias; proporcionar detalles de la respuesta después de un incidente; alertar a las partes interesadas afectadas; y asegurar una coordinación y comunicación apropiada.

Por su parte las Normas Técnicas para la gestión y control de las Tecnologías de Información del MICITT[30] establecen que la institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas.

Dado lo anterior, es importante que el Ministerio de Hacienda determine la necesidad de comunicación de las actividades de recuperación con las partes interesadas proporcionando detalles de la respuesta que se dio, del estado de los sistemas de información y de lo que resta de la recuperación, para que con ello se logré el acceso oportuno a la información y la toma de decisiones pertinente. Lo anterior debido a lo siguiente:

---

27 Oficio DGH-179-2022 Consideraciones preliminares ante la pérdida de las colas de información del sistema de gestión documental (ePower) de la División de Adeudos Estatales, de fecha 18 de agosto de 2022.
28 Informe Técnico sobre encriptación de unidad de información no estructurada del sistema ePower, de octubre de 2022.
29 Punto 8.4.1 Generalidades y el Punto 8.4.3 Advertencia y comunicación de la Norma INTE/ISO 22301:2020 Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio - Requisitos, segunda edición del 30 de abril de 2020.
30 Punto XIII Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos del 10 de noviembre de 2021.

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

a) A nivel interno del Ministerio de Hacienda[31] se desconocen los protocolos para la operación durante la contingencia y no se han comunicado formalmente las acciones que se realizan para la restauración de los sistemas y/o servicios de la DTIC. Los funcionarios de la DTIC describieron la comunicación como escasa, muy restringida, inoportuna y contradictoria; y la coordinación como deficiente entre los equipos emergentes.
b) Por su parte, el 55% de los encargados funcionales de los sistemas en las Direcciones del Ministerio señalaron[32] que no han tenido información oportuna de los procesos realizados por el Ministerio en términos de la recuperación.
c) A nivel externo, se consultó[33] a once instituciones sobre la satisfacción con la oportunidad de la información que suministró el Ministerio de Hacienda durante el período en que los sistemas no estuvieron activos y en el período en que se habilitaron los mismos. Al respecto, en promedio se obtuvo una calificación de 6 (En un rango 1 y 10, donde 10 es totalmente satisfecho).

   Con respecto del nivel de satisfacción se indicó que la información fue entregada tardíamente, las instrucciones fueron giradas de manera informal y a veces contradictorias. Adicionalmente, indicaron que los plazos no consideraban la capacidad real de respuesta de las instituciones, y los tiempos de atención para los incidentes reportados fue prolongado y/o no respondido.

Dado todo lo anterior, es importante gestionar una adecuada comunicación y coordinación con las partes interesadas proporcionando detalles de la respuesta que se dio y de lo que resta de la recuperación, para que con ello se logré el acceso oportuno a la información y la continuidad de los servicios a un nivel aceptable, así como, para la toma de decisiones oportunas.

Firmado digitalmente por JULISSA SAENZ LEIVA
Fecha: 2023-02-01 07:32

Julissa Sáenz Leiva
Gerente del Área de Fiscalización para el Desarrollo de las Finanzas Públicas

[31] Información recopilada mediante entrevista con los encargados directos de los sistemas de información, bases de datos, servidores, redes y respaldos.
[32] Información recopilada mediante encuesta realizada a los encargados funcionales.
[33] Se consultó a once instituciones con el objetivo de conocer los controles implementados durante el período del 18 de abril al 15 de noviembre de 2022, la actualización de la información y la percepción sobre la información brindada por el Ministerio de Hacienda durante el período de contingencia. (Ministerio de Obras Públicas y Transporte; Ministerio de Salud; Ministerio de Hacienda; Ministerio de Seguridad Pública; Poder Judicial; Consejo Nacional de Vialidad; Ministerio de Justicia y Paz; Ministerio de Trabajo y Seguridad Social; Registro Nacional; Dirección Nacional de Centros de Educación y Nutrición y de Centros Infantiles de Atención Integral; y el MInisterio de Educación)

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica