AUDITORÍA INTERNA
INSTITUTO NACIONAL DE SEGUROS

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA EVALUACIÓN DE LOS PLANES DE: CONTINUIDAD DE NEGOCIO (BCP) Y RECUPERACIÓN DE DESASTRES DE TECNOLOGIAS DE INFORMACIÓN (DR)

IA-028-2022
28 DE JULIO DE 2022

RESUMEN EJECUTIVO

La presente revisión se originó en cumplimiento del Plan Anual de trabajo 2022, como parte del cual, y con sustento en la valoración de riesgos realizada, se consideró relevante evaluar los planes de continuidad del negocio (BCP) y recuperación de desastres de tecnologías de información (DR), dada su importancia para el negocio.

Para contextualizar, conviene indicar que la Institución cuenta con un plan de continuidad del negocio que gestiona la Dirección de Riesgos junto con otras acciones y coordinaciones para atender eventos de gran impacto, sin dejar de lado el plan de recuperación de desastres específico para mantener la continuidad operativa de la infraestructura tecnológica que está bajo la responsabilidad de la Dirección de Tecnologías de Información.

La revisión es relevante y de carácter especial por su vinculación con el negocio y la infraestructura tecnológica e incluyó la verificación de la aplicación de sanas prácticas que rigen la materia, para establecer si están acordes con la realidad Institucional y si cumplen el cometido de ofrecer resiliencia ante eventos que afecten la normalidad de las operaciones de acuerdo con la información obtenida al 30 de junio de 2022.

Durante la revisión se detectaron las siguientes situaciones:

1. Personal del Grupo INS sin cumplimentar la capacitación de Fundamentos de la Continuidad del Negocio.
2. Contactos de los miembros de los equipos desactualizados en los planes de continuidad del negocio (BCP) y recuperación de desastres (DR).

Estas situaciones exponen a los riesgos de: a) “Comunicación” y “Continuidad” ya que parte de la población Institucional falta de recibir la capacitación en continuidad lo que puede afectar las acciones a realizar en los procesos críticos o vitales en caso de un evento, y con ello impactar la disponibilidad de los servicios, debido al desconocimiento sobre cómo actuar en estos casos, b) “Eficiencia” al no tener la información actualizada de los miembros que conforman los equipos de los planes de continuidad del negocio y recuperación de desastres, lo que posibilita el retraso y eventual duplicidad de esfuerzos al momento de accionarlos.

Sobre estos aspectos, se formulan recomendaciones para las Direcciones de Riesgos y Tecnologías de Información, que a criterio de esta Auditoría deben ponerse en práctica para mitigar la exposición a los riesgos identificados.

Tabla de contenido

IA-028-2022
28 de julio, 2022

I. INTRODUCCIÓN

A. Origen del estudio

La presente revisión se originó en cumplimiento del Plan Anual de trabajo 2022, el cual, con sustento en la valoración de riesgos realizada, se consideró relevante evaluar los planes de continuidad del negocio (BCP) y recuperación de desastres de tecnologías de información (DR), dada su importancia para el negocio.

B. Objetivo general

Evaluar la razonabilidad de los planes de continuidad de negocio (BCP) y recuperación de desastres de tecnología de información (DR) mediante la verificación de la aplicación de sanas prácticas que rigen la materia, soportadas en un análisis de impacto de negocio (BIA), para establecer si están acordes con la realidad institucional y si cumplen el cometido de ofrecer resiliencia ante eventos que afecten la normalidad de las operaciones.

C. Objetivos específicos

1. Evaluar los planes de continuidad el negocio (BCP) y recuperación de desastres (DR) de Tecnologías de Información, mediante la revisión de los registros documentales e instrumentos utilizados, para identificar áreas de mejora en el proceso.

2. Evaluar los planes de continuidad del negocio (BCP) y recuperación de desastres de tecnología de información (DR), para determinar si están acordes con la realidad institucional, mediante le revisión de acciones planteadas dentro del proyecto Marco de Gestión Empresarial de Tecnologías de Información (MGETI) y los planes alternos de trabajo.

3. Verificar el Análisis de Impacto de Negocio (BIA), mediante su comparación con sanas prácticas que rigen la materia, para determinar su suficiencia ante eventos que afecten las operaciones.

D. Alcance del estudio

La revisión comprendió la evaluación de los planes de continuidad de negocio (BCP) y recuperación de desastres de tecnología de información (DR), con el propósito de establecer si se asegura razonablemente la continuidad de las operaciones y disponibilidad de los servicios, así como el involucramiento del personal responsable de su ejecución, mediante la revisión y análisis de dichos planes con corte al 30 de junio de 2022.

E. Metodología

Las actividades de la auditoría en torno al presente estudio fueron realizadas de conformidad con la normativa aplicable al ejercicio de la auditoría interna y en cumplimiento de las Normas Generales de Auditoría para el Sector Público.

La metodología aplicada involucró el uso de prácticas, técnicas y procedimientos de auditoría, tales como: a) consultas a funcionarios de las Direcciones de Riesgos (Unidad de Continuidad del Negocio)

y Tecnologías de Información (Operaciones y Servicios de Tecnología), b) inspección documental y c) consulta de normas internacionales, tales como la ISO 22301 “Seguridad y Resiliencia”.

F. Marco normativo

1. Ley General de Control Interno, Ley N° 8292.
2. Normas de control interno para el Sector Público, N-2-2009-CO-DFOE.
3. Marco Internacional Cobit 2019.

G. Comunicación de resultados

En cumplimiento de lo establecido en la norma 205.08 de las “Normas Generales de Auditoría para el Sector Público”, los resultados de este estudio fueron presentados en reunión celebrada por videoconferencia el 28 de julio de 2022, a la Gerencia, jefaturas de las Direcciones de Riesgos y Tecnología de Información, quienes manifestaron su conformidad con lo observado y sugerido.

H. Aspectos positivos determinados

Por parte de los clientes involucrados en la revisión se mantuvo una participación y apertura, durante las sesiones, donde reinó un ambiente cordial y sin reserva para suministrar la información.

I. Aspectos corregidos durante la ejecución del estudio

1. Durante la revisión se reactivó el curso Fundamentos de Continuidad del Negocio en la herramienta UCINS por solicitud de la Dirección de Riesgos dirigida a la Subdirección de Cultura y Talento.

2. Producto del seguimiento ofrecido al tema de “Interrupción del sistema de enfriamiento del Centro de Datos Principal” y la revisión interna que realizó la Subdirección de Servicios Generales Corporativos, se establecieron medidas de control preventivo y correctivo, de las cuales se citan las más relevantes a continuación (SDSGC-01062-2022):

    a. *Se revisó las ubicaciones de las cámaras de seguridad y capacitó al personal interno del Centro de Datos y proveedores que ofrecen servicios preventivos y de mantenimiento en este.*
    b. *Las actualizaciones de los servidores se seguirán realizando en coordinación con el personal del Centro de Datos y Tecnologías de Información para observar que todo ocurra de la manera correcta y que las mismas no coincidan con otros trabajos de los Centros de Datos.*
    c. *Se reportan las anomalías, alarmas o alertas a los compañeros de Tecnología de información filtrando las que no podrían llegar a comprometer la disponibilidad de los Centros de Datos.*
    d. *El centro de monitoreo de la dirección de tecnología de información monitorea en paralelo los Centros de Datos y el proveedor también realizará esta actividad de manera complementaria.*
    e. *Se incrementó de tres a cuatro rondas a los sistemas electromecánicos en los Centros de Datos, por turno de manera permanente.*
    f. *Se digitalizan las bitácoras de forma obligatoria, al finalizar el turno de cada colaborador y se enviará por correo al encargado del Centro de Datos con copia al buzón de monitoreo y el segundo ingeniero electromecánico con disponibilidad.*
    g. *Se realizo una reunión con los técnicos para recalcar la importancia de las rondas, reporte inmediato de incidencias, responsabilidades y labores de coordinación entre el personal de la Subdirección y Tecnologías de Información en el Centro de Datos.*

h. Se gestiona la promoción de un proceso de contratación para adquirir el servicio de administración de dicha infraestructura con un proveedor experimentado en dicha actividad, esto de conformidad con lo analizado en visita realizada al Banco Popular, y se incluirá el servicio de mantenimiento predictivo, técnico y de repuestos para atender imprevisto en tiempos óptimos.

II. RESULTADOS

Para contextualizar, conviene indicar que la Institución cuenta con un plan de continuidad del negocio que gestiona la Dirección de Riesgos junto con otras acciones y coordinaciones para atender eventos de gran impacto, sin dejar de lado el plan de recuperación de desastres específico para mantener la continuidad operativa de la infraestructura tecnológica que está bajo la responsabilidad de la Dirección de Tecnologías de Información.

Se determinó la existencia de acciones orientadas a formar y concientizar al personal de la Institución en el tema de Continuidad del Negocio, donde la Dirección de Riesgos desarrolló un curso denominado "Fundamentos de la Continuidad del Negocio", dirigido al Grupo INS con el fin de fortalecer el entendimiento y las capacidades del personal de las diferentes unidades administrativas en procura de reducir los efectos (impactos) adversos de un evento no deseado y procurar así, restablecer las operaciones en el menor tiempo posible.

También, se constató la existencia del Plan de Continuidad del Negocio (BCP), políticas y procedimientos que permiten orientar y coordinar las actividades de respuesta frente a diferentes escenarios identificados en los BIA generados para cada proceso institucional, para los cuales, la metodología de Manejo de Incidentes, el Programa y el Manual para la Gestión de continuidad del negocio del INS, el Plan de continuidad de negocio para eventos catastróficos o masivos y los Planes alternos de trabajo desarrollados, dirigen el accionar de la Unidad de Continuidad del Negocio, adscrita a la Dirección de Riesgos.

En cuanto al Plan de Recuperación de Desastres (DR), la Dirección de Tecnologías de Información cuenta con un Plan de Continuidad de las Tecnologías de Información y Comunicación (PCTIC), que guía las actuaciones de los diferentes equipos de recuperación en procura de minimizar el impacto de una interrupción en la infraestructura de TI. Complementan estas actividades, los procesos COBIT implementados: DSS02 Administración de incidentes de servicio y DSS03 Administración de problemas que incluyen cualquier afectación en la infraestructura crítica de la Institución y cuentan con roles y responsabilidades definidos, así como procedimientos oficializados.

Sobre la realización de pruebas (simulacros) de los sistemas contingentes, este Despacho revisó la totalidad de las pruebas ejecutadas desde enero 2021 a marzo de 2022, donde los resultados para cada uno de los simulacros realizados, se resume:

> *"El usuario final pudo verificar la funcionalidad y aplicación del sistema contingente de forma satisfactoria".*

Es importante indicar, que se presentaron situaciones como: problemas con el cambio de roles de bases de datos, réplica entre DNS externos intermitente, interfaz con SINPE, ajustes en los sistemas de Riesgos del Trabajo y Point General, que fueron solventados en el momento de las pruebas y que, por consiguiente, la funcionalidad de los contingentes derivó en resultados positivos.

Además, se confirmó que las áreas de negocios, Direcciones de Riesgos y Tecnologías de Información mantienen una estrecha relación para la elaboración, ejecución y revisión de los planes alternos, análisis de impacto del negocio, planes de continuidad y recuperación de desastres.

También, se conoció que actualmente existe un canal en la herramienta Teams, que vincula los responsables de los diferentes equipos de atención de eventos de continuidad y recuperación en aras de dar mayor agilidad al proceso de comunicación apoyados de otros medios de comunicación complementaria.

Cada uno de los planes de trabajo alternos, aprobados por la Gerencia una vez superada la revisión previa de la Dirección de Riesgos (quién corrobora la funcionalidad y ofrece sugerencias de mejora), permite contar con la información necesaria para orientar a cada área de negocio, acerca de las acciones a seguir en caso de que se de alguna interrupción que afecte de manera imprevista el proceso gestionado.

Del examen de los análisis de impacto de negocios (BIA), se obtuvo que se consideraron las sanas prácticas aplicables a la realidad institucional en su enfoque de procesos y que son fundamento para que la Unidad de Continuidad del Negocio del grupo INS, clasifique la criticidad de los subprocesos e infraestructura tecnológica de misión crítica.

En la documentación y procedimientos generados y oficializados, en apego a la normativa COBIT, por parte del proyecto MGETI para el proceso “DSS04 Gestión de la Continuidad”, se observó la incorporación de una definición de: roles, responsabilidades, planes de capacitación, ejecución de simulacros y prácticas de actuación de la Brigada Corporativa de cara a una interrupción que afecte las operaciones. También, se orienta sobre la comunicación que fluye hacia el personal a cargo del plan de recuperación, a quienes se les remite en detalle las tareas en ejecución y orden de prioridad para su conocimiento, ejecución y actualización de ser necesario.

Producto del examen de eventos contingentes presentados en el primer trimestre (enero a marzo) del año 2022, se observó el detalle, motivo y solución registrada para cada situación por los especialistas asignados, los cuales fueron solventados con oportunidad y, además, ninguno tuvo vinculación con un evento de ciberseguridad (hacking, ataques DDoS, ataques en la nube, etc.).

Sobre el tema de seguridad, se conoció que en diciembre del año 2021, se adicionó al Plan de continuidad de Tecnologías de Información y Comunicación (PCTIC) una “Guía de atención a incidentes de Ciberseguridad”, que incluye definiciones, recomendaciones, responsabilidades, medidas preventivas y una lista de dispositivos de prevención con que cuenta el INS en caso de presentarse algún evento relacionado a la ciberseguridad, sin dejar de mencionar las iniciativas contractuales que la Institución gestiona en torno a este tema.

Finalmente, no se omite mencionar que, durante la revisión, el 19 de febrero de 2022, se presentó una situación que afectó el Centro de Datos Principal debido a la suspensión del enfriamiento de los aires acondicionados, donde de acuerdo con los diferentes informes de la Subdirección de Servicios Generales, Departamento de Ingeniería y Mantenimiento, la Dirección de Tecnologías de Información y la empresa Electrotécnica (proveedor especialista contratado), arribaron a la siguiente conclusión:

> *“De manera concluyente de acuerdo con lo descrito anteriormente y a la evidencia adjunta en el informe, se determina que la alimentación eléctrica de los controladores que gestionan los sistemas de enfriamiento de ambos brazos de agua helada fue manipulada físicamente, apagando primero el*

controlador del brazo A y seis minutos después el controlador del brazo B. Al apagarse los controladores, provoca el apagado de los sistemas de agua helada de ambos brazos del centro de datos principal, coincidiendo esto con el ingreso del operador del INS a los cuartos eléctricos donde se ubican los controladores." Fuente: Oficio SDSGC-00402-2022

Al respecto, producto del seguimiento y consultas realizadas, se tomaron medidas preventivas y correctivas para evitar que la situación se vuelva a presentar, ver detalle en el punto anterior a "Resultados" de este informe. Además, se conoció que en oficio SDCT-01853-2022 del 22 de junio del 2022 la Subdirección de Cultura y Talento gestionó la solicitud de apertura de un procedimiento ordinario remitido a la Gerencia, la cual en oficio G-01482-2022 requirió a la Subdirección de Servicios Generales emitir un nuevo informe con mayor detalle y sustento sobre lo acontecido (G-01482-2022 del 6/04/2022).

No obstante, lo anterior se observó como aspectos de mejora los siguientes:

A. Personal del Grupo INS sin cumplimentar la capacitación de Fundamentos de la Continuidad del Negocio.

Se determinó que 957 (28,46%) de 3366 funcionarios no cumplieron de forma satisfactoria la capacitación del curso Fundamentos de la Continuidad del Negocio, lo que deja ver una falta de seguimiento sobre este programa de capacitación con el fin de que las personas que reprobaron o suspendieron la misma fueran motivadas a completarlo, así como también, asegurar que toda la población del Grupo INS fuera cubierta.

Contar con personal que desconoce sobre cómo se gestiona la continuidad del negocio, los procesos, canales de comunicación y equipos de trabajo establecidos para abordar eventos que pueden afectar las operaciones críticas del negocio, conllevan una eventual inacción y duplicidad de esfuerzos con impacto en la pronta disponibilidad de los servicios (riesgos de comunicación y continuidad).

Lo anterior incumple lo estipulado en el Manual para la Gestión de Continuidad del Negocio del INS que indica:

"VII Capacitación de Continuidad de Negocio
1. Fomentar el conocimiento de *todas las personas funcionarias del INS* sobre la continuidad de negocio y su importancia para la Institución."

B. Contactos de los miembros de los equipos desactualizados en los planes de continuidad del negocio y recuperación de desastres.

En los planes de continuidad y recuperación de desastres[1], dada su finalidad, es imprescindible que la información de los equipos de actuación esté debidamente actualizada con los datos necesarios para ubicar al personal en caso de presentarse una emergencia, esto por cuanto es un recurso vital para ponerlos en marcha cuando se requieren. Sin embargo, en la revisión se encontró que tanto en el Plan de Continuidad de Negocio como en el Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC) esta información se encuentra desactualizada.

[1] *Plan de Continuidad de Negocio, Manual para la Gestión de Continuidad del Negocio del INS, Plan de continuidad de negocio para eventos catastróficos o masivos, Plan de Continuidad de las Tecnologías de Información y Comunicación (PCTIC) y Planes alternos de trabajo.*

Lo anterior se debe a que los miembros de los equipos de los planes de continuidad y recuperación de desastres incluyen los nombres de los funcionarios entre otra información, lo que implica que, en cada movimiento interno de estos, se deba gestionar la respectiva actualización y aprobación de la Junta Directiva.

Tener información desactualizada conlleva que se pueda incurrir en confusión y por ende actuación desordenada de las personas en el momento de tratar de contactar a los equipos y activar dichos planes con la respectiva extensión en tiempo de recuperación (riesgo de "Eficiencia").

Esto contraviene lo estipulado en el Marco de referencia Cobit 2019 en el proceso DSS04 Gestionar la continuidad:

"DSS04.05 Revisar, mantener y mejorar el plan de continuidad.
4. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa, procesos de negocio, acuerdos de externalización, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones*".*

III. CONCLUSIONES

Una vez evaluados los planes de Continuidad del Negocio (BCP) y Recuperación de Desastres (DR) con que cuenta la Institución se observó la participación de las áreas de negocio involucradas, la aplicación de sanas prácticas acordes con la realidad institucional que, junto con las políticas, procedimientos, metodología, manuales y planes alternos de trabajo, contribuyen a hacer frente, de manera razonable a los eventos que afectan la continuidad. Con los productos del proyecto MGETI también, se contribuyó a fortalecer y asegurar la disponibilidad de los componentes tecnológicos de información de misión crítica según el escenario e impacto analizado en los "Análisis de Impacto de Negocio" (BIA) desarrollados para cada proceso, donde se tomó en cuenta la criticidad y área de negocio potencialmente afectada según el escenario revisado.

No obstante, se observó la necesidad de reforzar los aspectos de capacitación y actualización de los planes.

Situaciones que exponen a riesgos de: a) "Comunicación" y "Continuidad" ya que parte de la población institucional no ha realizado la capacitación en continuidad, lo que puede afectar las acciones a realizar en los procesos críticos o vitales en caso de un evento y con ello impactar la disponibilidad de los servicios, debido al desconocimiento sobre cómo actuar en estos casos, b) "Eficiencia" al no tener la información actualizada de los miembros que conforman los equipos de los planes de continuidad del negocio y recuperación de desastres, lo que posibilita el retraso y eventual duplicidad de esfuerzos al momento accionarlos.

IV. RECOMENDACIONES

IA-028-2022
28 de julio, 2022

Para la Gerencia General

Girar instrucciones a las direcciones de Riesgos y Tecnologías de Información, para que, en un plazo de 10 días hábiles a partir del recibo del presente informe, se elabore y remite a este Despacho el plan de acción para la atención de lo recomendado a continuación.

A. Para la Dirección de Riegos.

A.1 Gestionar con la Subdirección de Talento Humano la inclusión en el sistema de Gestión Virtual del Talento (GVT) dentro de la sección del "Plan individual de desarrollo" de cada colaborador de Casa Matriz, la obligatoriedad de llevar el curso de Fundamentos de Continuidad del Negocio contenido en la plataforma UCINS.

Prioridad: Media.

A.2 Evidenciar la actualización y aprobación de la nueva versión del plan de continuidad del negocio (BCP) que actualiza los puestos sin alusión a los nombres de los funcionarios que conforman los equipos de atención de eventos.

Prioridad: Alta.

B. **Para la Dirección de Tecnologías de Información.**

B.1 Evidenciar la actualización y aprobación de la nueva versión del Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC) que actualiza los puestos sin alusión a los nombres de los funcionarios que conforman los equipos de atención de eventos.

Prioridad: Alta.

Hecho por:

AMALIA PATRICIA CHINCHILLA MONGE (FIRMA)
Firmado digitalmente por AMALIA PATRICIA CHINCHILLA MONGE (FIRMA)
Fecha: 2022.07.28 15:39:03 -06'00'

Licda. Amalia Chinchilla Monge, MAP
Auditor I de Tecnologías de Información

Revisado y aprobado por:

ADRIAN CHAVARRIA MORA (FIRMA)
Firmado digitalmente por ADRIAN CHAVARRIA MORA (FIRMA)
Fecha: 2022.07.28 15:45:32 -06'00'

Lic. Adrián Chavarría Mora, CISA
Supervisor de Auditoría de
Tecnologías de Información

RICARDO ARTURO DE LOS ANGELES ARCE SANDI (FIRMA)
Digitally signed by RICARDO ARTURO DE LOS ANGELES ARCE SANDI (FIRMA)
Date: 2022.07.28 15:34:26 -06'00'

Lic. Ricardo Arce Sandí, CISA
Jefe de Auditoría de Tecnologías de Información