Resumen Ejecutivo

Esta Auditoría Interna contrató a la empresa DATASOFT con el objetivo primordial de realizar un diagnóstico del estado actual, recabando evidencia suficiente y pertinente para valorar la efectividad de los procesos de la continuidad que aseguran la continuidad del negocio de CONAPE, enfocándose en la información y los procesos críticos de la empresa y sin dejar de lado la aplicación de las mejores prácticas de la industria como lo son en este caso las normas ISO 22301 e ISO 27031.

Cada uno de los hallazgos encontrados se clasifican según resultado de la evaluación de la evidencia de auditoría frente a los criterios de auditoria definidos por la norma ISO 19011, a saber: Conformidad, Observación, No conformidad menor, No conformidad mayor; ésta última identifica las áreas con mayor oportunidad de mejora, en las cuales se recomienda actuar de inmediato por los niveles de afectación que tienen para la función de la seguridad dentro de la Institución.

El estudio permitió identificar aspectos tales como: CONAPE cuenta con una estructura de procesos muy bien lograda; no se han definido objetivos específicos pertinentes que sean medibles, congruentes con la política de continuidad del negocio y que sean comunicados a las distintas partes interesadas; se identifica que la función de la Sección de Informática está subordinada al Departamento de Planificación lo que le impide tener su independencia y por tanto el poder de decisión, coordinación y comunicación con la alta dirección de forma tal que se puedan entender, implementar y gestionar adecuadamente los requisitos de continuidad del negocio; se halló que la información documentada en el SGCN no es suficiente según los requisitos de la norma ISO 22031 ya que debe evidenciarse claramente los servicios o productos que CONAPE debería ofrecer a su público meta, así como sus requisitos y niveles mínimos de entrega en caso de un evento de contingencia, incluyendo las dependencias que existe uno de otros o bien como parte de una cadena de suministros incluidos los proveedores; se identifica la carencia de un sistema de gestión de servicios de tecnologías de información alineados con la estrategia y macroprocesos y que reúna los requisitos de la información en un Sistema de Gestión de Servicios; en el sistema de gestión BCM Doc, sección Planeación, apartado Contexto de la organización no se tiene documentado las partes interesadas relativas al SGCN y sus respectivos requisitos (incluso aquellos de carácter legal o reglamentario), además se deben documentar las exclusiones o aquellos procesos, actividades que no serán cubiertos por el SGCN y la razón por la cual no afecta a CONAPE en un ambiente de contingencia; pese los esfuerzos de comunicación y concientización en que se ha incurrido, se determina mediante la aplicación de instrumento tipo cuestionario que el 25% de los encuestados dicen no conocer de algún documento que funcione como Política de Continuidad de Negocio que dicte como mínimo las responsabilidades de los grupos de recuperación y los funcionarios en general y su compromiso con la continuidad y que a su vez haya sido publicado o comunicado formalmente en la Institución; no se han definido ni documentado las responsabilidades del Grupo de Apoyo Administrativo y del Grupo de Trabajo en Contingencia; se definieron los requerimientos de competencias para el perfil del Coordinador de Continuidad de Negocio, sin embargo no se le ha proporcionado la capacitación planificada y requerida en el documento Organización de Continuidad de Negocio; no se han registrado en el BCM Doc las actividades de capacitación impartida a los miembros de la organización brindadas con la intención de asegurar las competencias requeridas para cumplir con los objetivos de continuidad; se obtiene evidencia de

implementación de actividades de concientización durante los últimos dos años, sin embargo, estas actividades son esfuerzos aislados que no fueron enmarcados dentro de un plan formal de concientización, además, no hay más registros de evidencia de despliegue de sensibilización durante los últimos seis meses previos a este estudio; el encargado de la actualización de los planes y procedimientos de comunicación es el funcionario Jean Carlo Mejías, no obstante, en la herramienta BCM Doc figura con esta responsabilidad Mario Porta García; se detecta que solo hay 37 usuarios activos en la herramienta BCM Doc lo que presenta un 50% de la totalidad de la población de funcionarios; no se cuenta con un procedimiento formal y documentado para la gestión y acceso a la información documentando del SGCN; en la herramienta BCM Doc, sección Implementación, apartado Gestión de Riesgos, al igual que en el análisis BIA, se detecta que existen una gran cantidad de riesgos que no han sido revisado y actualizados durante el último año; se identificó que el tiempo de recuperación objetivo (RTO) corresponde a 4 horas concluyéndose muy optimista respecto de la realidad de CONAPE con base en la estrategia planteada; en la sección Implementación, apartado Estrategias de Continuidad hay 2 estrategias (4 y 6) que tiene documentadas varias alternativas de implementación (de 3 a 4 alternativas) y no hay claridad sobre los recursos necesarios para la alternativa finalmente seleccionada; durante visita al sitio alterno de trabajo ubicado en el Centro Corporativo El Tobogán, se logran identificar deficiencias respecto a lo pactado en el cartel de contratación, además se identificó que "La solicitud de alquiler de Sala para Días NO Programados la realizará el Administrador del Contrato, con mínimo 4 horas de antelación al inicio del alquiler" lo que le da la posibilidad al proveedor de disponer de la sala de trabajo hasta 4 horas después de dicha solicitud, momento en el cual el personal de CONAPE estaría apenas ocupando la sala e iniciando con la preparación en sitio alterno y por tanto este escenario impediría el cumplimento del tiempo promedio de recuperación según el BIA que es de 4 horas; se carece de una política de teletrabajo implementada que faculte al personal ejercer sus actividades desde una ubicación remota sin la necesidad de trasladarse al sitio principal de trabajo; la estrategia de continuidad presenta algunas debilidades identificadas durante la revisión de los resultados de las pruebas y ejercicios, incluyendo el último realizado el día 24 de agosto de 2018 apoyado también en Informe sobre el simulacro Centro alterno de operaciones Licitación Pública No. 2015LN-000001-01 documentado por la Auditoría Interna; los acuerdos de nivel de servicio con proveedores considerados como críticos deben ser validados debido a que por ejemplo el acuerdo de nivel de servicio de la Empresa Logística Transaccional del Istmo (LTI) no es congruente con el tiempo objetivo de recuperación establecido en el BIA y además no incluye el sitio alterno de trabajo como uno de los lugares donde se debería prestar el servicio de esta empresa que colabora en la resolución de incidencias que se pudieran presentar con el módulo STX de conectividad a los Bancos de Costa Rica y Banco Nacional durante una contingencia y se detectó que precisamente las entidades bancarias antes mencionadas no están identificadas como proveedores críticos y no existen acuerdos de nivel de servicios firmados con estas partes interesadas clave para los servicios de pago en línea que ofrece CONAPE; el personal de CONAPE que trabaja directamente con los procesos o funciones críticas no posee los procedimientos impresos; pese a que se definieron archivos y herramientas de recuperación tales como instructivos de trabajo, éstos no han sido identificados como registros vitales de los procesos críticos de CONAPE de manera que no es posible asegurar su disponibilidad en caso de contingencia; no hay evidencia de ejecución de ejercicios integrales que evalúen toda la capacidad operacional, la efectividad de los procedimientos de continuidad y la respuesta del personal de CONAPE ante un evento disruptivo que ponga a prueba la integración de las

actividades de todos los planes; todos los esfuerzos realizados a la fecha como parte de los ejercicios de prueba no están documentados en un plan formal de las pruebas del BCP; en el BCM Doc, sección Mejoramiento, apartado Acciones correctivas las mismas se han actualizado principalmente con base en ejercicios y pruebas previamente realizadas, sin embargo, éstas poseen registro de acciones correctivas que no han sido aplicadas; no existe información documentada de qué, cómo y cuándo se desea medir el desempeño y efectividad del SGCN y por ende tampoco de los informes de resultados como evidencia de mediciones anteriores; no hay una asignación formal de responsabilidades para la Auditoría Interna en el documento Organización de Continuidad de Negocio; no está actualizado el BCP para que se identifique claramente dónde (tanto centro de recuperación tecnológica ubicado en ADN Datacenter en Alajuela como en el centro alterno de trabajo ubicado en centro el Tobogán, San José) se realizará la recuperación, así como también las distintas partes involucradas en el proceso de recuperación incluyendo los proveedores críticos que interactúan; el Plan de Continuidad no aborda todos los posibles escenarios que pudiesen afectar las operaciones tomando en consideración que éstas dependen de la documentación física que se gestiona en las instalaciones, mismas que pueden ser afectadas parcialmente o en su totalidad (en el peor de los escenarios); los procedimientos manuales en su mayoría se apoyan en otros registros o documentación electrónica como por ejemplo instructivos detallados, sin embargo, no tienen documentado cómo se gestionarán (quien, cómo, cuándo, dónde) estos registros; el Plan de Continuidad no precisa en los procedimientos administrativos de logística, traslado, suministros requeridos para iniciar las labores de recuperación desde el sitio alterno de trabajo; no existe un proceso o plan para retornar las operaciones al sitio principal una vez que haya terminado el incidente disruptivo de forma que se realice una evaluación del sitio afectado, se limpie el sitio y restaure la infraestructura (en caso de ser requerido), se restauren los servicios de TI en el sitio principal y se traslade la operación a la actividad normal; el Formulario de Registro de Incidentes no permite registrar toda la información requerida sobre el posible incidente disruptivo (de conformidad con ISO 22301) y su evaluación posterior; se carece de procedimientos de apagado seguro y cierre de las instalaciones; respecto al plan de emergencias no hay claridad total en el personal respecto de a quién deben notificar primero para activar el sistema de emergencias interno y algunos no están familiarizados con los términos como por el ejemplo el concepto de “zona de amortiguamiento”; de la revisión del Plan de Comunicaciones y sus procedimientos se concluye que CONAPE cuenta con la documentación requerida por la norma ISO 22301; el Coordinador del Plan de Recuperación ante Desastres no ha recibido toda la capacitación requeridas según el PCN, CONAPE no cuenta con una política específica para el PTCN; no se han documentado los proveedores críticos del PTCN; no se han establecido los procedimientos de continuidad de TIC para responder ante cualquier evento disruptivo y cómo continuará o recuperará sus actividades dentro de un tiempo establecido en el BIA; del plan DRP se indica que el Equipo de Recuperación Tecnológica no requiere transporte, sin embargo, es claro que en la estrategia de activación del plan este equipo debe trasladarse al centro alterno de trabajo; El plan PTCN adolece de elementos importantes como la logística que se refiere a cómo se adquieren o consiguen, transportan y mantienen los recursos, así como también los requerimientos de seguridad de los servicios de tecnologías de información que se deben recuperar. Finalmente, para cada uno de los hallazgos se establecieron las respectivas recomendaciones y la asignación de responsables.