Informe Definitivo de Auditoría

NOMBRE DEL PROCESO	**GESTIÓN DE CONTINUIDAD DE NEGOCIO**
LÍDER DE PROCESO	**GERMAN ARMANDO CORREA AMADO** Jefe Oficina Asesora de Planeación y Sistemas
AUDITORES	**VILMA LEONOR GARCÍA PABÓN** Asesora de Control Interno (E) **JULIE ANDREA FANDIÑO PATIÑO** Contratista (Apoyo) **JHON WILLIAM RUIZ RUBIO** Profesional Universitario (E)
FECHA DE AUDITORIA	Noviembre de 2021

OBJETIVO DE LA AUDITORIA

Realizar seguimiento a la Gestión de Continuidad de Negocio implementada en la Entidad acorde con los planes, programas, procedimientos y normas técnicas establecidas, así mismo, al avance y cumplimiento de las acciones de mejora suscritas con la Superintendencia Financiera de Colombia

ALCANCE DE LA AUDITORIA

Acciones y actividades descritas anteriormente durante el periodo comprendido entre el 01 de enero al 30 de septiembre de 2021

CRITERIOS DE LA AUDITORIA

- NTC – ISO 22301:2019. Seguridad y resiliencia. Sistema de Gestión de continuidad de negocio. Requisitos
- GTC – ISO 22313:2019. Seguridad de la sociedad. Sistema de gestión de continuidad de negocio. Guía
- GTC – ISO/IEC 27031:2016 tecnología de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de información y las comunicaciones para la continuidad de negocio
- GTC-ISO 22317:2017 Seguridad de la sociedad. Sistemas de gestión de la continuidad de negocio
- Resolución Interna 0311 del 11 de junio de 2021 *"Por la cual se crea el Comité Estratégico de Continuidad del Negocio en el Fondo de Previsión Social del Congreso de la República – FONPRECON"*

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

FICHA TÉCNICA (Herramientas utilizadas, universo, población, objeto, marco estadístico)

- Se revisó la pertinencia de la estructura del Plan de Gestión de Continuidad de Negocio teniendo en cuenta la norma técnica NTC-ISO 22301 y la GTC-ISO 22313
- Se verificó la elaboración y construcción de los siguientes planes: para la comunicación, sensibilización y capacitación de seguridad de la información y continuidad de negocio; de gestión de crisis; y preparación de tecnología para la continuidad de negocio - IRBC
- Se evaluaron los 4 procedimientos de Continuidad de Negocio revisando la efectividad de cada uno de los controles, tiempos, responsables, registros y formatos correspondientes a cada uno de ellos
- Se evaluó la ejecución y cumplimiento de las acciones de mejora suscritas con la Superintendencia Financiera de Colombia

EJECUCIÓN PROCESO AUDITOR

I. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

En el desarrollo de sus operaciones, las organizaciones, públicos o privadas, pueden enfrentarse a distintas amenazas tales como incendios, terremotos, fallos de tecnología, brotes pandémicos e incluso atentados terroristas a sus instalaciones físicas y/o a su infraestructura tecnológica; al enfrentar todas estas amenazas se pueden originar complicaciones e interrupciones que pueden involucrar la imposibilidad de continuar con misión de la Entidad o presentar pérdidas económicas, y lo que es peor aún, perdida de vidas humanas o afectarlas considerablemente.

Para la GTC-ISO 22313:2019 la continuidad de negocio es: "*la capacidad de la organización para continuar suministrando productos o servicios a niveles predefinidos aceptables, posteriormente a un incidente de interrupción. La gestión de la continuidad de negocio (BCM, por sus siglas en inglés) es el proceso de lograr la continuidad de negocio, y hace referencia a cómo una organización aborda los incidentes de interrupción que de otra forma podrían impedir el logro de sus objetivos*".

Para demostrar el compromiso de la Alta Dirección con la implementación de la continuidad de negocio en la Entidad, se ha cumplido con lo dispuesto en el numeral 5.3 de la GTC-ISO 22313:2019 al establecer una Política de continuidad del negocio, la cual se encuentra señalada dentro del documento PLN-GTC-001 cómo parte del capítulo 7.

Adicionalmente, y en cumplimiento del numeral 5.4 de la GTC-ISO 22313:2019, se ha conformado un Comité Estratégico de Continuidad del Negocio a través de la Resolución 0311 del 11 de junio de 2021. Este Comité tiene por Secretario Técnico al Profesional Responsable de la Unidad de Riesgo Operativo y como Coordinador al Jefe de la Oficina Asesora de Planeación y Sistemas.

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

PLAN DE CONTINUIDAD DE NEGOCIO

El Plan de Continuidad de Negocio se encuentra formalizado dentro del Sistema de Gestión de Calidad ISO 9001:2015 con código PLN-GTC-001 actualizado a la versión 8 del 25 de junio de 2021, esto alineado con los estándares ISO y del Modelo de Seguridad y Privacidad de la Información de la Entidad.

La implementación de este Plan obedece a lo dispuesto en el numeral 6.2 de la GTC-ISO 22313 que dice: "*Se debería elaborar un plan para crear y gestionar la BCM*…", y con el literal a del numeral 8.1 de la misma guía: "*(…) establecimiento de un plan de implementación y acordando una metodología adecuada para la implementación de la BCM; (…)".*

El documento señala tres objetivos en el marco de continuidad del negocio que son:

- Adoptar estrategias de continuidad de negocio, para asegurar el restablecimiento de la operación de la Entidad desde cada uno de sus procesos con sus tareas y procedimientos priorizados, ante la ocurrencia de eventos disruptivos que afecten la obtención de los resultados esperados, para el cumplimiento de los objetivos misionales.
- Preparar a la Entidad lo mejor posible, mediante la identificación y gestión de recursos, personas, bienes, activos, medios y servicios suficientes, necesarios y disponibles para operar en contingencia y preservar la confianza en los pensionados, afiliados y demás grupos de interés.
- Mantener un PCN coordinado, actualizado y alineado a estándares ISO, buenas prácticas y marco de cumplimiento, dentro de una estrategia de mejora continua

La estructura que desarrolla el documento se encuentra basada en lo dispuesto por el numeral 8.4.4.3 de la NTC-ISO 22301, siendo la siguiente:

Capítulo	Criterio de norma técnica
3. Alcance del plan	Literal a del numeral 8.4.4.3 de la NTC-ISO 22301, Numeral 4.3.2 del GTC-ISO 22313
4. definiciones 5. Marco de referencia 6. Marco legal y de reglamentación	Numeral 4.2.2 de la NTC-ISO 22301, Numeral 4.2.2 de la GTC-ISO 22313
7. Política de continuidad de negocio	Numeral 5.3 de la GTC-ISO 22313, Numeral 5.2 de la NTC-ISO 22301
8. Roles y responsabilidades	Numeral 5.4 de la GTC-ISO 22313
9. Contexto de Fonprecon	Numeral 4.1 de la GTC-ISO 22313, Numeral 4.1 y 4.2 de la NTC-ISO 22301
10. Revisión, actualización y socialización del plan	Numeral 7.5 y Numeral 6.2 de la GTC-ISO 22313

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

11. Formación	Numeral 7.2 y 7.3 de la NTC-ISO 22301, Numeral 7.2 de la GTC-ISO 22313
12. Actividades operacionales priorizadas	Numeral 8.3.1 de la GTC-ISO 22313
13. Activos, bienes y servicios	Numeral 8.3 de la GTC-ISO 22313
14. Análisis de riesgos e impacto al negocio BIA	Numeral 8.2 de la GTC-ISO 22313, Numeral 8.2 de la NTC-ISO 22301
15. Gestión de incidentes	Numeral 8.4.2 de la GTC-ISO 22313
16. Comunicación	Numeral 8.4.3.2 de la GTC-ISO 22313
17. Gestión de crisis	Numeral 8.4.2 de la GTC-ISO 22313
18. Estrategia de continuidad de negocio	Numeral 8.3 de la GTC-ISO 22313. Numeral 8.3 de la NTC-ISO 22301
19. Seguridad y bienestar de la persona	Numeral 8.4.4.3.3 de la GTC-ISO 22313
20. Preparación de tecnologías de la información – IRBC	ISO 27031 y numeral 8.4.4.3.6 de la GTC-ISO 22313
21. pruebas periódicas al PCN	Numeral 8.5.3 de la GTC-ISO 22313
22. Monitoreo, medición, análisis y evaluación del plan	Numeral 9.1 de la GTC-ISO 22313, Numeral 9.1 de la NTC-ISO 22301
23. Auditoría interna	Numeral 9.2 de la GTC-ISO 22313
24. Mejora continua	Numeral 10.2 de la GTC-ISO 22313

Se observa que los capítulos del Plan de Continuidad de Negocio integran los numerales de las normas técnicas de referencia para la implementación de la Gestión de Continuidad de Negocio.

PLAN PARA LA COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO

El plan se encuentra formalizado dentro del Sistema de Gestión de Calidad con código PLN-GTC-006 actualizado a la versión 2, esto para poder integrar la temática de continuidad de negocio en el titulo y contenido del documento. El objetivo del documento es aplicar temáticas que concienticen al personal y fortalezca las actividades priorizadas en el marco de la gestión de continuidad de negocio.

La implementación de este Plan cumple con lo establecido en el numeral 7.2 de la GTC-ISO 22313:2016 que reza: "*La organización debería establecer programas de capacitación y toma de conciencia para todos los empleados que se pueden ver afectados por un incidente de interrupción, y exigir a los contratistas que trabajan en su nombre, demostrar que la(s) persona(s) que llevan a cabo el trabajo bajo su control tienen la competencia requerida para el BCMS, y los roles que tendrán en una respuesta*". Lo anterior puede verse cumplido a través del desarrollo del capitulo 6,

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

debido al establecimiento de los temas que permitirán desarrollar las competencias necesarias en el marco de la continuidad de negocio.

PLAN DE GESTIÓN DE CRISIS

El plan de gestión de crisis permite a la Entidad abordar eficazmente situaciones de emergencia reales y percibidas cuando éstas surjan. Se encuentra formalizado dentro del SGC con código PLN-GTC-007 y estando en la primer versión del plan con fecha del 25 de junio de 2021.

Este documento tiene por objeto establecer, operar y mejorar los recursos necesarios para el manejo de la crisis para que la entidad pueda tomar el control de las situaciones adversas.

Hallazgo No. 1 - Información de contacto incompleta y con datos de personal de carácter temporal

Dentro del punto 6.2 en el que se describe las personas, entidades o grupos a los cuales se debe contactar en caso de crisis, se encuentra información incompleta, además de encontrarse datos de contacto que corresponden a personal con carácter temporal dentro de la Entidad, lo cual dificultaría en caso de crisis la comunicación con el equipo encargado para su manejo.

Se recomienda ajustar el plan en el punto 6.2 con información de contactos adecuada que permita el enlace eficaz en caso de crisis para su manejo, de conformidad con lo descrito en la GTC-ISO 22313 numeral 8.1.5 inciso e: "*el personal recibe soporte y las comunicaciones adecuadas en caso de una interrupción*."

PLAN DE PREPARACIÓN DE TECNOLOGÍA PARA LA CONTINUIDAD DE NEGOCIO – IRBC

El documento se encuentra formalizado dentro del SGC con código PLN-GTC-008 encontrándose en la versión 1 del plan. El objetivo del plan es establecer tiempos, elementos y estrategias que respondan a interrupciones de los servicios tecnológicos o de cualquiera de los activos de tecnología, con el fin de proteger y recuperar las funciones críticas del negocio que se puedan ver comprometidas como resultado de la manifestación de diversos incidentes.

La Oficina de Control Interno reviso el Plan de Tecnología para la Continuidad del Negocio encontrando que se encuentra ajustado a lo mencionado por la NTC-ISO 22301

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

en su numeral 8.4.4, adicionalmente a lo señalado en el numeral 8.4.4.3.6 de la GTC-ISO 22313.

PROCEDIMIENTOS

La adopción de procedimientos relativos a la implementación, mantenimiento y mejora de la Gestión de Continuidad de Negocio en FONPRECON cumple con lo estipulado en el numeral 8.4.1 de la NTC-ISO 22301 que reza: "*La organización debe implementar y mantener esquemas de respuesta que permitan una advertencia oportuna y la comunicación a las partes interesadas relevantes. Debe brindar planes y procedimientos para gestionar la organización durante una interrupción. Los planes y procedimientos deben usarse cuando se requieren activar las soluciones para la continuidad de negocio*".

Adicionalmente, se tiene en cuenta lo establecido con el numeral 8.4.1 de la GTC-ISO 22313 que señala: "*La organización debería implementar y documentar procedimientos que brinden un control general de la respuesta a un incidente de interrupción y debería reanudar actividades dentro de sus tiempos objetivo de recuperación…"*

Teniendo en cuenta todo lo anteriormente mencionado, la Entidad dispone de procedimientos, formalizados debidamente en el Sistema de Gestión de Calidad, que permiten abarcar el desarrollo de la Gestión de Continuidad de Negocio.

PROCEDIMIENTO PARA REPORTAR INCIDENTES DE CIBERSEGURIDAD

El procedimiento se encuentra formalizado en el Sistema de Gestión de Calidad con código PRO-GTC-013 y actualizado a la versión 2, esto para alinear con la Circular Externa 033 de 2020 de la Superintendencia Financiera de Colombia.

El documento tiene por objetivo de establecer los parámetros y acciones necesarias para el reporte de incidentes relacionados con ciberseguridad acorde con los protocolos designados para la materia.

El criterio normativo tenido en cuenta para el procedimiento incluye: ISO/IEC 27032:2012, Ley 599 de 2000, Ley 1273 de 2009, Resolución 3066 de 2011, CONPES 3701 de 2011, Circular Externa 029 de 2014, Decreto 1078 de 2015, CONPES 3854 de 2016, Circular Externa SFC 007 de 2018 y Circular Externa SFC 033 de 2020.

El desarrollo de las actividades inicia con la recolección de la evidencia que soporte el incidente ocurrido, continua con el reporte del incidente a la Superintendencia Financiera. Se finaliza con el reporte del incidente al Comité estratégico para la continuidad de negocio.

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

PROCEDIMIENTO GESTIÓN DEL CAMBIO

El procedimiento se encuentra formalizado en el Sistema de Gestión de Calidad con código PRO-DEI-007 con una única versión, la de lanzamiento del 18 de junio de 2021. El objetivo del documento establecer las condiciones para adoptar los cambios que afecten al Sistema de Gestión de Calidad en la Entidad.

El criterio normativo tenido en cuenta para el procedimiento incluye: NTC-ISO 22301:2019, GTC 281:2017, GTC-ISO-IEC 27031:2016, GTC-ISO-TS 22317:2017, NTC-ISO 22313:2019, NTC ISO 9000:2015 y NTC ISO 9001:2015.

El desarrollo de actividades comienza con la identificación de los cambios significativos que puedan afectar la gestión de calidad, continua con la documentación del cambio y el propósito de este. Finaliza con la verificación, por parte del responsable del cambio, de verificar que las modificaciones se encuentran debidamente implementadas y en ejecución.

PROCEDIMIENTO PARA EVALUACIÓN DEL DESEMPEÑO DEL PLAN DE CONTINUIDAD DE NEGOCIO

Su objetivo es establecer los criterios para la formulación y seguimiento de los indicadores para evaluar el desempeño del plan de continuidad de negocio de la entidad de acuerdo con lo exigido en la Guía Técnica Colombiana GTC-ISO 22313:2016.

Su versión 1 fue creada el 28/09/2021, con código PRO-GTC-018, inicia con el establecimiento de indicadores de nivel estratégico en el Plan de Continuidad del Negocio y culmina con las auditorias al PCN.

La Oficina de Control Interno considera que los indicadores planteados dentro del procedimiento cumplen con los criterios de medición, monitoreo y evaluación que presenta la GTC-ISO 22313 en sus numerales 8.1.4 y 9.1.

PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES

Su objetivo principal es establecer las actividades, condiciones, controles y decisiones necesarias para identificar, analizar, gestionar, documentar, actualizar y comunicar de manera oportuna y eficiente los incidentes, emergencias o desastres como eventos que puedan afectar la normalidad de las operaciones. La implementación de este procedimiento obedece con lo dispuesto en los numerales 8.4.2 y 8.4.3 de la GTC-ISO 22313

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

Su versión 1 fue creada el 26/06/2021, con código PRO-GTC-017, inicia con la designación del equipo de gestión de incidentes y culmina con la descripción de las actividades con sus responsables y el documento de registro.

EJERCICIOS SOBRE CONTINUIDAD DE NEGOCIO

Considerando lo señalado por el numeral 8.5.1 de la GTC-ISO 22313: "*Los procedimientos y medidas de continuidad de negocio de una organización no se pueden considerar confiables sino hasta que se lleven a cabo ejercicios y se mantenga su vigencia. Los ejercicios son esenciales para asegurar que las estrategias, políticas, planes y procedimientos que se han implementado son adecuados y cumplen con los objetivos de continuidad de negocio".* En cumplimiento de lo anterior, el área auditada ha dado a conocer, mediante memorando 20212200026933, el Cronograma de Pruebas y Ejercicios del Plan Preparación de Tecnología para la Continuidad de Negocio -IRBC, este documento proyecta la realización de 20 actividades para los meses de octubre y noviembre de 2021 resaltando las siguientes acciones:

- Borrar una de las bases de datos Recuperar y restaurar copia desde repositorio de contraloría general de la nación
- Desconectar el canal principal de internet y observar si de forma automática entra en operación el canal de internet de respaldo
- Simular ciber ataque
- Restaurar copia de servidor de base de datos en ambiente de pruebas con red interna

Al final de la ejecución de los ejercicios planteados, se pretende realizar un informe sobre los resultados y lecciones aprendidas. Adicionalmente, se tiene el cronograma Pruebas Tecnológicas en el marco del Plan de Continuidad de Negocio con la cual se abarcará los ejercicios de recuperación de los sistemas tecnológicos de Fonprecon a través de las siguientes acciones principales:

- Recuperación de servidor de dominio principal, servidor de dominio secundario, servidor de bases de datos, Estación de trabajo Windows, servidor de aplicación, servidor de presentación
- Instalación de Nómina de Pensionados (ZBOX), Cartera (ZBOX), Contabilidad (ZBOX), Tesorería (ZBOX), Afiliaciones (ZBOX), Recurso Humanos (ZBOX), QCD, ORFEO y OwnCloud
- Recuperar y comprobar servidor de correo institucional

Con la realización de estos ejercicios se cumple con lo dispuesto por el numeral 8.5 de la GTC-ISO 22313. Adicionalmente, teniendo presente la respuesta por parte del auditado: "*(…)desde el alcance de Gestión Tecnológica esta es una actividad que se*

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

realiza una vez al año en el mes de noviembre…", se cumple con lo dispuesto en el numeral 8.5 de la NTC-ISO 22301 que dice: "*La organización debe implementar y mantener un programa de ejercicios y pruebas para validar a lo largo del tiempo la eficacia de sus soluciones y estrategias para la continuidad de negocio".*

II. ACCIONES DE MEJORA SUSCRITAS CON LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

En vista de las recomendaciones realizadas por la Superintendencia Financiera de Colombia, en el marco de revisión de la Gestión de Continuidad de Negocio, esto teniendo en cuenta el numeral 3.1.3.1 de la Circular Externa 041 de 2007, se establecieron una serie de acciones de mejora para cumplir con lo recomendado por el ente de control. A continuación, se presenta el avance de las actividades señaladas por la Oficina Asesora de Planeación y Sistemas:

Recomendaciones	Breve descripción de las medidas adoptadas	Fecha de inicio	Fecha de cierre	Avance	Observaciones control interno
Considerar en la planificación, implementación y mantenimiento del PCN, las buenas prácticas, normas, metodologías, modelos, estándares nacionales o internacionales como referencia para la mejora continua.	1. Adquirir versiones actualizadas de estándares ISO, en materia de continuidad de negocio 2. Socializar al equipo de trabajo involucrado en PCN, temáticas en materia de continuidad de negocio: * Estándares ISO * Guía 10 MSPI * Circular 007 de 2018 SFC	31/05/2021	25/06/2021	100%	La Oficina de Control Interno evidenció la adquisición de las siguientes Normas Técnicas correspondientes a la Gestión de Continuidad del Negocio: NTC ISO 22301:2019|, GTC-ISO-IEC 27031, GTC-ISO-TS 22317 y NTC ISO 22313, además del soporte correspondiente al Plan de Continuidad del Negocio COD:PNL-GTC-001 V8.
El área encargada del PCN debe reportar a la Junta Directiva, la Alta Gerencia y a los distintos comités de la Entidad los resultados de su gestión de forma periódica.	Se adopta el comité estratégico para continuidad de negocio, en donde se establece a la Oficina Asesora de Planeación y Sistemas como responsable de reportar a las instancias del caso, los resultados de la gestión del PCN	20/05/2021	11/06/2021	100%	La Oficina de Control Interno evidenció que mediante Resolución 0311 de 11 de junio de 2021 la creación del Comité Estratégico de Continuidad del Negocio, su conformación, sesiones y cuórum.
Identificar y gestionar los recursos, bienes, activos, medios y servicios suficientes, necesarios y disponibles para operar en contingencia.	Mesas de trabajo con resultado de matriz que documenta los recursos, alineados a las estrategias de continuidad, los procesos, los diferentes escenarios adversos y otros como las variables RTO, RPO, MTD	1/07/2021	30/09/2021	100%	Se soportó la implementación de la recomendación realizada, mediante el archivo llamado Estrategias PCN - consolidado por procesos.xlsx las reuniones de las mesas de trabajo con cada área.

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

Evaluar y alinear las estrategias de continuidad del negocio con los requerimientos de la SFC, los cambios normativos, los procesos, escenarios, y las actividades críticas del negocio.	Mesas de trabajo con resultado de matriz que documenta los recursos, alineados a las estrategias de continuidad, los procesos, los diferentes escenarios adversos y otros como las variables RTO, RPO, MTD	1/07/2021	30/09/2021	100%	Se soportó las reuniones de las mesas de trabajo ajustando las necesidades de cada área al PCN, mediante el archivo llamado "Estrategias PCN - consolidado por procesos.xlsx".
Definir e implementar la estrategia considerada para la indisponibilidad de las sedes físicas, cumpliendo con las condiciones necesarias para seguir prestando el servicio de forma oportuna.	Mesas de trabajo con resultado de matriz que documenta los recursos, alineados a las estrategias de continuidad, los procesos, los diferentes escenarios adversos y otros como las variables RTO, RPO, MTD	1/07/2021	30/09/2021	100%	Se soportó la implementación de la recomendación realizada, mediante el archivo llamado Estrategias PCN - consolidado por procesos.xlsx las reuniones de las mesas de trabajo con cada área.
Complementar, adaptar y transformar planes y estrategias de continuidad de negocio para hacer frente a cambios climáticos y ambientales.	Se aborda la temática y se documenta en el capítulo 10.1 del plan “Preparación de tecnología para la continuidad de negocio - IRBC"	1/07/2021	30/09/2021	100%	Se presenta mediante soporte el Plan de Preparación de Tecnología para la Continuidad del Negocio- IRBC en su versión 1 creada el 28/07/2021, dónde se documentan los recursos técnicos, humanos y logísticos necesarios para la categorización, planeación y pruebas de los activos tecnológicos, las alternativas de contingencia, así como la recuperación de desastres tecnológicos
Definir, ejecutar y medir el cumplimiento del plan de capacitación y sensibilización de Continuidad del Negocio, el cual debe orientarse a todo el personal de la Entidad.	Integrar capítulo para continuidad de negocio, con alcance para personas, contratistas y proveedores dentro del plan de capacitación y sensibilización en seguridad, incluyendo entre otros las temáticas contenidas en el numeral 7.3 del estándar GTC-ISO 22313	1/06/2021	17/06/2021	100%	La Oficina de Control Interno evidenció que el Plan para la Comunicación , Sensibilización y Capacitación de Seguridad de la Información y Continuidad del Negocio, se encuentra actualizado integrando todo el personal de la entidad incluyendo contratistas y proveedores.
Evaluar y mejorar los ciclos, contenidos y actividades adicionales de los programas de formación y sensibilización para avanzar en metas, habilidades y competencias de continuidad, así como verificar la apropiación de planes y estrategias	Se identifican las diferentes audiencias y temáticas y se documentan en el plan respectivo. Se integra capítulo para medición del aprovechamiento	1/06/2021	17/06/2021	100%	La Oficina de Control Interno observó que dentro del Plan para la Comunicación , Sensibilización y Capacitación de Seguridad de la Información y Continuidad del Negocio, se encuentran identificadas las diferentes audiencias y temáticas, además de ser documentadas en el plan respectivo, además de la inclusión de la medición y el aprovechamiento para medir

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

en todos los niveles jerárquicos de la Entidad.					la comprensión del auditorio con respecto del tema impartido.
Contemplar dentro del proceso de gestión de cambios la actualización y prueba oportuna del PCN y el BIA considerando las novedades en el contexto de la organización, los ajustes realizados a los procesos críticos, los riesgos emergentes y las modificaciones a la plataforma tecnológica, entre otros aspectos.	Se adopta procedimiento de gestión del cambio V1, integrando el alcance indicado en esta recomendación	1/06/2021	25/06/2021	100%	Se evidencia por parte de Oficina de Control Interno la adopción del procedimiento Gestión del Cambio V1 aprobado con fecha 18/06/2021.
Revisar, actualizar y divulgar toda la documentación y componentes del PCN al menos una vez al año o por cambios, modificaciones o incidentes.	Dentro del Comité Estratégico de Continuidad del Negocio, se integra la función: 7)Identificar temáticas y planear la capacitación y sensibilización transversal en Continuidad del Negocio. En el PCN, se incluye capítulo:	1/06/2021	25/06/2021	100%	Se verificó que el Plan de Continuidad del Negocio se publicara dentro del Sistema de Gestión de Calidad de la Entidad quedando a disposición de todos los funcionarios de la entidad.
Definir, evaluar y actualizar métricas e indicadores a nivel estratégico, táctico y operativo, para los controles, metas y objetivos de continuidad del negocio (ERP, DRP, PCN, capacitación, pruebas) y promover la mejora continua.	Se diseñan indicadores y se documenta en procedimiento de evaluación de desempeño	1/07/2021	30/09/2021	100%	Se evidenció el cumplimiento de la recomendación mediante el "Procedimiento evaluación del desempeño PCN v1" que establece los conceptos básicos, características principales y orientaciones de seguimiento a los indicadores de gestión de continuidad de negocio
Optimizar los tiempos y mecanismos de replicación de datos utilizados entre el CPD y el CAPD para asegurar su disponibilidad y recuperación.	Se está abordando para el siguiente reporte	1/07/2021	31/12/2021	0%	Se encuentra en proceso de implementación.

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

Evaluar el cumplimiento de las normas de sismo resistencia y certificaciones, para ubicaciones físicas críticas, como centros de cómputo, oficinas principales, centros de operación alternos, entre otros. De igual forma exigirlo para sus proveedores críticos.	Se escala consulta a la administración del edificio World Service, donde Fonprecon ocupa los pisos 2 y 3. Se mantendrá seguimiento en las asambleas de administración del edificio, donde Fonprecon es propietario de los pisos 2 y 3	24/06/2021	25/06/2021	100%	Se presenta consulta realizada a los administradores del edificio World Service, informando que se les dará seguimiento a las asambleas sobre el tema de sismo resistencia de la edificación.
Medir de forma regular y periódica el nivel de madurez de continuidad del negocio de la entidad, utilizando como referencia las escalas y criterios suministrados en la circular externa 033 de 2020, el modelo Capability Maturity Model (CMM), o el modelo Business Continuity Maturity Model (BCMM).	Se adopta el modelo Capability Maturity Model (CMM), para medir el grado de madurez del PCN, agregando el capítulo respectivo en el PCN v8	3/06/2021	25/06/2021	100%	Se registra el cumplimiento de la recomendación dentro del Plan de Continuidad del Negocio V8 en el Capitulo 25 llamado Modelo de Medición de Madurez dónde se adopta el modelo Capability Maturity Model (CMM), para medir el grado de madurez del PCN
El Comité de Auditoría deberá monitorear y reportar el cumplimiento de los planes de acción definidos por la Entidad para remediar los hallazgos indicados por la AI sobre la gestión de continuidad de negocio y las pruebas ejecutadas.	Se adopta Comité estratégico para continuidad de negocio, con los roles definidos para monitorear y reportar el cumplimiento de los componentes del PCN. Se solicita a control interno incluir en sus planes de auditoria	20/05/2021	24/06/2021	100%	Se evidenció mediante la adopción del Comité Estratégico de Continuidad del Negocio definiendo los roles para monitorear y reportar el cumplimiento de los componentes del PCN y la inclusión por parte de la Oficina de Control Interno dentro del Plan de Auditorias anual.
Fortalecer los programas y planes de trabajo de AI incluyendo actividades para evaluar la efectividad y eficiencia del PCN, la idoneidad de los criterios aplicados en el BIA, los RTO y los RPO, y la integridad de las estrategias para soportar los servicios críticos de la Entidad.	Se integra un comité de trabajo que representa a todos los procesos, con roles bien definidos, para gestión, seguimiento y mantenimiento de los componentes PCN. Se solicita a control interno incluir en sus planes de auditoria	20/05/2021	24/06/2021	100%	Se evidenció mediante la adopción del Comité Estratégico de Continuidad del Negocio definiendo los roles para monitorear y reportar el cumplimiento de los componentes del PCN y la inclusión por parte de la Oficina de Control Interno dentro del Plan de Auditorias anual.
Contar con un procedimiento definido para identificar, analizar,	Se adopta procedimiento de gestión de incidentes V1	1/06/2021	25/06/2021	100%	Se cuenta con la adopción del Procedimiento para la Gestión de Incidentes V1 con fecha de aprobación el

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

EJECUCIÓN PROCESO AUDITOR

gestionar, documentar, actualizar y comunicar los incidentes o eventos de manera oportuna y eficiente.					25/06/2021
Tipificar los eventos, incidentes y criterios de activación de crisis. Así mismo, designar grupos de respuesta competentes acorde a la clasificación realizada.	Se adopta plan para la gestión de crisis V1, donde se incluyen las recomendaciones.	10/06/2021	21/06/2021	100%	Se cuenta con el Plan de Gestión de Crisis V1 con fecha de aprobación el 25/06/2021, dónde se establece las consideraciones para la activación e inactivación de crisis dentro de la Entidad.
Garantizar el adecuado funcionamiento y gestión de la cadena de suministros y el cumplimiento de las obligaciones de terceros para el cumplimiento de los servicios.	La Entidad lo realiza según el procedimiento denominado Adquisición de bienes y servicios V9	1/06/2021	15/06/2021	100%	Se cuenta con el Procedimiento de adquisición de Bienes y Servicios V9 con fecha de actualización el 22/02/2021. Cuyo objeto es establecer las actividades, condiciones, controles y decisiones necesarias, para efectuar la adquisición de bienes y servicios.
Identificar, seleccionar, gestionar y evaluar de forma periódica los proveedores, así como sus riesgos, estrategias, atención, acuerdos, contratos, con el fin de garantizar la prestación de los servicios.	La Entidad realiza este alcance mediante el procedimiento denominado Adquisición de bienes y servicios v9	1/06/2021	18/06/2021	100%	Se cuenta con el Procedimiento de adquisición de Bienes y Servicios V9 con fecha de actualización el 22/02/2021. Cuyo objeto es establecer las actividades, condiciones, controles y decisiones necesarias, para efectuar la adquisición de bienes y servicios.

Fuente: Oficina Asesora de Planeación y Sistemas

Las recomendaciones impartidas por la Superintendencia Financiera de Colombia se encuentran hasta el corte de solicitud de información, 30 de septiembre de 2021, en un avance promedio del 95%; se encuentra pendiente la ejecución de las acciones de mejora de una recomendación.

OBSERVACIONES

Hallazgo No. 1 - Información de contacto incompleta y con datos de personal de carácter temporal

PLAN DE MEJORAMIENTO

Se solicita que cada una de las observaciones comunicadas, deben incluirse en el plan de mejoramiento a suscribir, contemplando acciones preventivas y correctivas para los

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA

casos mencionados y así subsanar las observaciones presentadas. Los tiempos para la realización de dichas actividades deberán ser cortos. La Oficina Asesora de Planeación y Sistemas, como área auditada, deberá construir y consolidar el Plan de Mejoramiento dentro de los 10 días hábiles siguientes a la fecha de la entrega del presente informe definitivo y enviarlo a Control Interno para su suscripción. Para la presentación del Plan de Mejoramiento se deberá utilizar el formato F05-PROCIG-001, incluido en el Sistema de Gestión de la Calidad, Procedimientos Control Interno a la Gestión

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA
Cra. 10 No. 24-55 Piso 2o. y 3o. ■ Tel.: 3415566 Fax: 2863396 ■ www.fonprecon.gov.co ■ BOGOTA D.C. - COLOMBIA