INFORME 15A DE 2023
EVALUACIÓN AL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)
PERÍODO AUDITADO DEL 01 DE MAYO DE 2022 AL 31 DE MAYO DE 2023

1. OBJETIVO GENERAL

Evaluar y verificar por parte de la Oficina de Control Interno (OFCIN) de la Caja Promotora de Vivienda Militar y de Policía (CPVMP), la efectividad y cumplimiento en la administración del Plan de Continuidad del Negocio (PCN) incluyendo la evaluación de los elementos para prevenir y atender emergencias, administración de escenarios de crisis, planes de contingencia y capacidad de retorno a la operación normal, de acuerdo con lo requerido por la SFC en el Capítulo XXIII en la CBCF (CE 100 de 1995), las modificaciones realizadas a través de la CE 025 de 2020, numeral 3.1.3.2, las demás modificaciones y/o actualizaciones pertinentes.

1.1 Objetivos Específicos

- Evaluar el cumplimiento en la Administración del PCN en la Caja Promotora de Vivienda Militar y de Policía (CPVMP).
- Verificar que se le esté dando cumplimiento a las normativas internas y externas que regulan la administración y manejo del PCN.
- Identificar recursos y procesos priorizados para la recuperación de las operaciones.
- Identificar que se cuente con los planes, procedimientos y en general con la documentación necesaria para la gestión de crisis y del DRP.
- Verificar que se estén realizando pruebas y actualizaciones relacionadas con los resultados de las pruebas al PCN.
- Identificar las reglas o actividades generales para asegurar una adecuada recuperación de información y servicios.

2. ALCANCE

Evaluar el cumplimiento del PCN, de acuerdo con lo establecido por la SFC, políticas internas de la CPVMP descritas en el Manual de Gestión del PCN código GR-NA-MA-008, versión 5 del 26-05-2022, Manual de Seguridad de la Información y Ciberseguridad código GR-NA-MA-009, versión 3 del 25-06-2021, Plan de Recuperación ante Desastres – DRP código IT-NA-PL-003 versión 5 del 14-02-2022, Guía Análisis del Impacto del Negocio – BIA, código GR-NA-GU-028 versión 5 del 13-02-2023, Guía del Usuario Punto Alterno de Continuidad – PAC código GR-NA-GU-005 versión 11 del 13-02-2023, Norma ISO 22301:2012 Gestión de la continuidad de negocio, y demás normatividad aplicable para la evaluación del cumplimiento en la administración del PCN, durante el periodo del 01 de mayo de 2022 al 31 de mayo de 2023.

3. METODOLOGÍA

Para el desarrollo de los objetivos de auditoría descritos, el equipo auditor realiza un requerimiento inicial de información tanto a la OAGRI como a OAINF, con el fin de hacer un diagnóstico inicial del cumplimiento normativo del PCN, y de las políticas internas establecidas para su gestión durante el periodo auditado.

4. MARCO LEGAL

4.1. Normatividad Externa

- Ley 87 de 1993 "por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones".

- Capítulo XXIII en la CBCF (CE 100 de 1995), las modificaciones realizadas a través de la CE 025 de 2020 y el Numeral 2.10 Plan de Continuidad del Negocio, normatividad expedida por la SFC, así como las demás modificaciones y actualizaciones pertinentes.

- Ley 973 de 2005, reglamentación que modifica la normatividad por la cual fue creada la Caja Promotora de Vivienda Militar y de Policía, artículo No 2, "*NATURALEZA. La Caja Promotora de Vivienda Militar y de Policía, es una Empresa Industrial y Comercial del Estado de carácter financiero del orden nacional, organizada como establecimiento de crédito, de naturaleza especial, dotada de personería jurídica autonomía administrativa y capital independiente, vinculada al Ministerio de Defensa Nacional y vigilada por la Superintendencia Bancaria.",* hoy Superintendencia Financiera de Colombia.

- Circular Externa 041 del 29-06-2007 de la SFC, numeral 3.1.3.1 Administración de la Continuidad del Negocio, en la que se determinan las medidas que permitan asegurar la Continuidad del Negocio.

- Circular Externa 052 del 24-10-2007 de la SFC Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios.

- Circular Externa 042 del 04-10-2012 de la SFC, por medio de la cual se incorporan algunas modificaciones al Capítulo Décimo Segundo del Título Primero de la Circular Básica Jurídica, en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones.

- Norma ISO 22301:2012 Gestión de la continuidad de negocio, norma internacional para la gestión de la continuidad de negocio y se ha desarrollado para ayudar a las empresas a minimizar el riesgo del tipo de interrupciones.

- Norma ISO 27001:2013 Gestión de Seguridad de la Información Anexo A numeral 17. Aspectos de Seguridad de la Información de la Gestión de continuidad de Negocio.

- Circular externa 029 de 2014 de la SFC, Parte I instrucciones generales aplicables a las entidades vigiladas Título I, Aspectos Generales Capítulo IV: sistema de control interno, Titulo II, Capítulo I: Canales, Medios, Seguridad y Calidad en el Manejo de Información en la Prestación de Servicios Financieros

- Decreto 1078 de 26-05-2015 Sector de Tecnologías de Información y las Comunicaciones, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá **601 755 7070**
Línea gratuita nacional **01 8000 185 570**
www.cajahonor.gov.co - **contactenos@cajahonor.gov.co**
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

- Decreto 648 de 2017 “por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública”.

- Decreto 1499 de 2017 “por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”, versión 3 y 4 MIPG.

- Norma ISO 31000: 2018 “Gestión del Riesgo”.

- Circular Externa 007 del 05-06-2018 de la SFC, Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.

  Ley 1952 de 2019 aplicable desde el 01-07-2021 para lo concerniente en Conflicto de Interés.

- Ley 1979 de 2019, en donde se establece que los Veteranos de la Fuerza Pública podrán ser afiliados voluntarios de la CPVMP para servicios financieros.

- Resolución 604 del 09-12-2019 “Por medio de la cual se actualiza la reglamentación del Comité Directivo de Continuidad y de los equipos de trabajo provisionales para la puesta en marcha del Plan de Continuidad del Negocio de la Caja Promotora de Vivienda Militar y de Policía”

- Circular Externa 008 del 17-03-2020 de la SFC, por la cual, la Superintendencia adopta medidas para garantizar la adecuada prestación del servicio en un entorno altamente digital, como medida de prevención, contra la propagación del COVID -19.

- Decreto 076 de 2022, por medio del cual se modifica la estructura de la Caja Promotora de Vivienda Militar y de Policía.

- Decreto Ley 353 de 1994 modificado por la Ley 973 de 2005 y la Ley 1305 de 2009.

- Decreto 1900 del 06-09-2013 por el cual se modifica la estructura de la CPVMP, dentro de la cual se determinan las funciones de sus dependencias y se dictan otras disposiciones.

- Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, V5, 2023.

4.2. Normatividad Interna

- Acuerdo 05 del 30-08-2016 “Por el cual se adopta el Estatuto Interno de la Caja Promotora de Vivienda Militar y de Policía”.

- Acuerdo 02 del 28-08-2020 “Por medio del cual se modifica el Acuerdo que regula los modelos de solución de vivienda, se unifican las disposiciones de afiliación y de servicios financieros ofrecidos por la Caja Promotora de Vivienda Militar y de Policía, y se dictan otras disposiciones.

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá 601 755 7070
Línea gratuita nacional 01 8000 185 570
www.cajahonor.gov.co - contactenos@cajahonor.gov.co
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

- Acuerdo 01 del 29-01-2021, que modifica al Acuerdo 02 de 2016 y deroga al Acuerdo 01 de 2017, actualiza las disposiciones que regulan el funcionamiento del Comité Financiero y Comité de Riesgos de la CPVMP.

- Acuerdo 02 del 28-05-2021 "por el cual se establecen las condiciones generales y financieras del Crédito Hipotecario de la Caja Promotora de Vivienda Militar y de Policía y se dictan otras disposiciones".

- Resolución 342 del 18-06-2021 (implementa el Acuerdo 02 de 2021).

- Resolución 084 del 02-02-2022, por la cual se actualizan y unifican las disposiciones que regulan la estructura, funciones y siglas de las Áreas y Grupos Internos de Trabajo de la Caja Promotora de Vivienda Militar y de Policía y se dictan otras disposiciones.

✓ **Documentación interna en la CPVMP a evaluar durante la presente auditoría:**

PCN:

- Guía Análisis del Impacto del Negocio - BIA, código GR-NA-GU-028 versión 4 del 17-01-2020.
- Guía Análisis del Impacto del Negocio - BIA, código GR-NA-GU-028 versión 5 del 13-02-2023 (Actual).
- Guía del Usuario Punto Alterno de Continuidad – PAC, código GR-NA-GU-005 versión 10 del 20-08-2020.
- Guía del Usuario Punto Alterno de Continuidad – PAC, código GR-NA-GU-005 versión 11 del 13-02-2023 (Actual).
- Manual de Seguridad de la Información y Ciberseguridad, código GR-NA-MA-009, versión 3 del 25-06-2021.

- Manual de Gestión del Plan de Continuidad del Negocio GR-NA-MA-008, código versión 5 del 26-05-2022.
- Manual de Gestión del Plan de Continuidad del Negocio GR-NA-MA-008, código versión 6 del 25-04-2023 (Actual).
- Matriz de Riesgos Plan de Continuidad, versión 1 de 20-04-2023.

- Plan de Recuperación ante Desastres – DRP, código IT-NA-PL-003 versión 5 del 14-02-2022.

5. DESARROLLO PROCEDIMIENTOS DE AUDITORÍA PCN PERÍODO AUDITADO DEL 01 DE MAYO DE 2022 AL 31 DE MAYO DE 2023

5.1. Seguimiento a las recomendaciones y observaciones del informe anterior.

En el Informe de Auditoría No. 18A de 2022 Evaluación al Plan de Continuidad del Negocio (PCN) período auditado del 01 de octubre de 2021 al 31 de octubre de 2022, se identificaron 2 oportunidades de mejora y 2 recomendaciones las cuales a la fecha de

elaboración del presente informe se encuentran pendientes de ejecutar con plazo máximo hasta el 31-Ago-2023, tal como se muestra en la siguiente imagen:

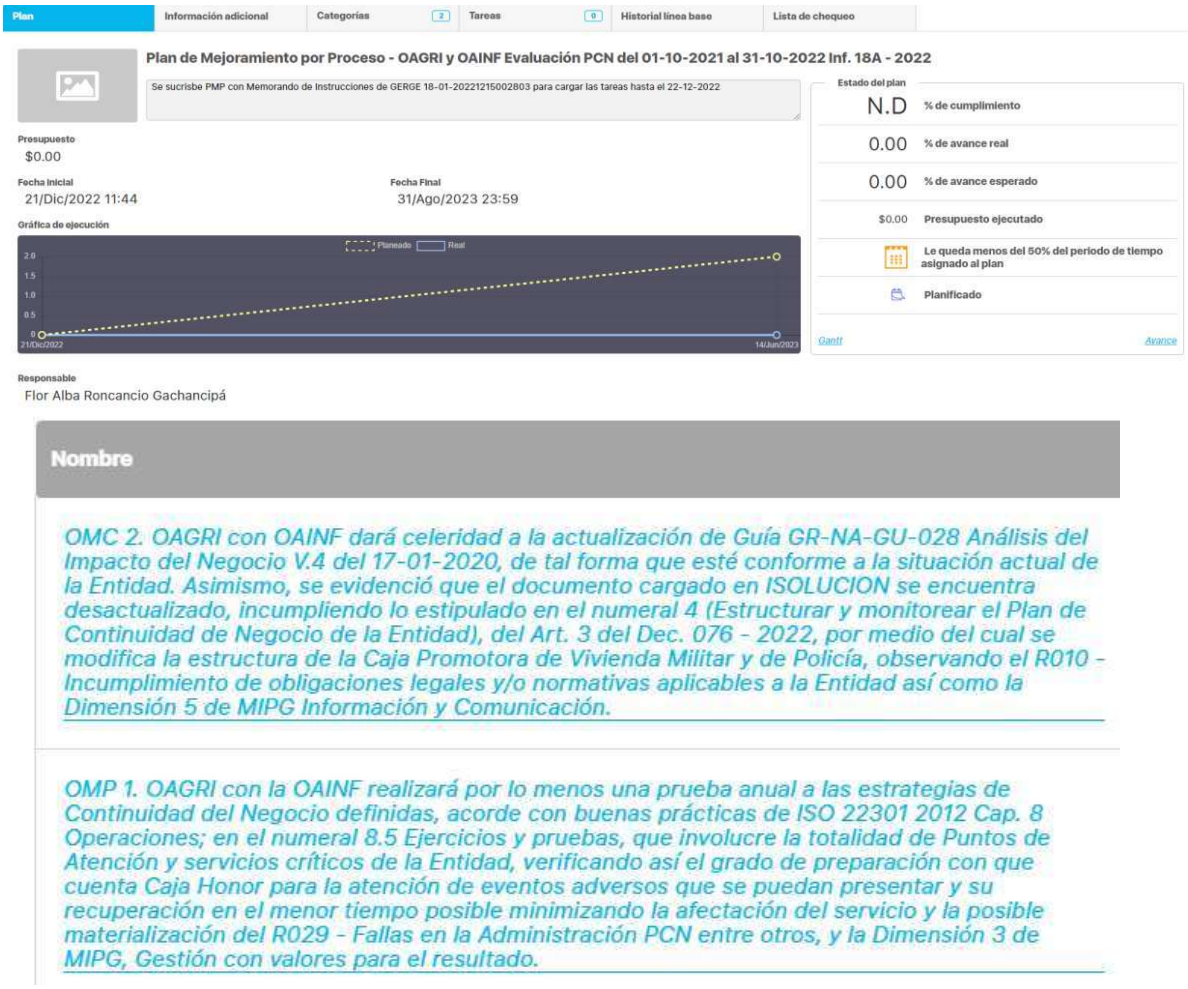

Figura 1. Evidencias Plan de Mejoramiento por Proceso - OAGRI Auditoría PCN Informe 18A - 2022.
Fuente: Planes - Suite Visión Empresarial Consultado 13-06-2023

5.2. Respuestas recibidas de la solicitud de información.

Teniendo en cuenta el requerimiento realizado el pasado miércoles 31 de mayo de 2023, a las jefaturas de OAGRI y a OAINF, es de anotar que la OAGRI mediante email de fecha 05-06-2023 indica que dispuso la información en el Repositorio Documental SharePoint, como se muestra a continuación:

Figura 2 Correo Respuesta solicitud requerimiento_25-11-2022.
Fuente: Correo electrónico.

Igualmente la OAGRI suministró la siguiente plantilla de Excel con observaciones de cada uno de los ítems de información PCN requerida por la OFCIN, así:

PLAN DE CONTINUIDAD DEL NEGOCIO – PCN	SHARE POINT	ENTREGADA	PENDIETE	OBSERVACION
1. Informes de resultados de las pruebas de continuidad y contingencia efectuadas en el periodo antes citado		5/06/2023		Se envía resultado del simulacro realizado para el 2022, está programada para el mes de junio de 2023 realizar el primer simulacro que es el de página y portales web
2. Documentos relacionados con el proceso de pruebas:				
Árbol de llamadas (Personal responsable indicando nombres y cargo, Nro. Contacto)		5/06/2023		se envía árbol de llamada
Minutograma del desarrollo de la prueba		5/06/2023		Se envía minutograma para el simulacro de Pagina y portales web , con los soportes requeridos
Comunicados a partes interesadas		5/06/2023		
Alcance de la prueba		5/06/2023		
Descripción de Escenarios de la prueba		5/06/2023		
Evidencias de comunicación en todo el proceso de pruebas		5/06/2023		
3. Planeación simulacro de contingencia y continuidad vigencia 2023		5/06/2023		Información confidencial
4. Política de Plan de Continuidad de Continuidad del Negocio		5/06/2023		Información confidencial
5. Guía Análisis del Impacto del Negocio		5/06/2023		Información confidencial
6. Plan de Recuperación de Desastres		5/06/2023		Se documento se encuentra en proceso para ser subido a ISOLUCION , para su actualización , se deja soporte de los correos para validar la gestión del proceso
7. Evidencias del presupuesto asignado para el PCN				Se solicito a la Oficina de OAINF , está pendiente por entrega

Figura 3 OAGRI – Plantilla Excel con observaciones de entrega de información
Fuente: Correo Electrónico 5-06-2023

5.3. Revisión de información por parte de la Oficina de Control Interno

5.3.1. Revisión de la información relacionada

Se valida en ISOLUCION la información publicada relacionada con el Plan de Continuidad de Negocio evidenciando, que la información soportada se encuentra actualizada de acuerdo como se observa a continuación:

Figura 4 Documentos Plan de Continuidad del Negocio.
Fuente: ISOLUCION, Consultado 14-06-2023

Plan de Recuperación Ante Desastres DRP, código IT-NA-PL-003 V 006 de fecha aprobación 08-06-2023

La OFCIN verificó el documento Plan de Recuperación Ante Desastres DRP, código IT-NA-PL-003, V 006 de fecha aprobación 08-06-2023 frente a la V5 del mismo documento, observando que fue actualizado en aspectos relacionados con la Matriz de Riesgo del DRP, descripción de Escenarios de Riesgos Operacionales y Aplicativos Críticos, Acuerdo de Niveles de Servicio establecidos con el proveedor Claro.

Sin embargo, la OFCIN hace especial énfasis respecto a que se tenga en cuenta las recomendaciones 4 y 5 documentadas en el anterior ejercicio auditor mediante Informe No. 18A de 2022, relacionada con:

"**Recomendación 4**: La OFCIN recomienda a OAGRI documentar en el árbol de llamadas los cargos específicos del personal involucrado en el ejercicio, y en la planeación previa del simulacro se documente de forma específica el árbol de llamadas con cargos, nombres y número de contacto de las personas encargadas del proceso; dando cumplimiento al Numeral 7.5 Información Documentada del Standard ISO 27001:2013 Seguridad de la Información, además de la Dimensión 5° Información y Comunicación de MIPG."
"**Recomendación 5**: La OFCIN recomienda a OAGRI y OAINF incluir en el documento IT-NA-PL-003 Plan de Recuperación ante Desastres – DRP, versión 5 con fecha de aprobación del 14-02-2022, se describan entre otros, los aspectos relacionados con los Acuerdos de Niveles de Servicios establecidos con cada uno de los proveedores con los cuales Caja Honor tiene servicios tercerizados, que se relacionen con el DRP y PCN, validando así ciertos criterios de calidad del servicio. Lo anterior, de tal forma que se dé cumplimiento al Numeral A.17 Aspectos de Seguridad de la Información de Continuidad de Negocio del Anexo A del Standard ISO 27001:2013 y a la Dimensión 3° Gestión con Valores para resultados de MIPG, además de la guía de buenas prácticas para la gestión de servicios de tecnologías de la información ITIL 4."

GR-NA-GU-028 Guia Análisis del Impacto del Negocio V4 del 17-01-2020

Con respecto al documento BIA, la OFCIN al consultar con fecha 16-03-2023 el repositorio documental ISOLUCION:

Figura 5 Guía Análisis de Impacto del Negocio
Fuente: Repositorio Documental Isolucion – Consultado 16-06-2023

observó que la versión oficial es V5 del 13-02-2023, no obstante, el documento suministrado por OAGRI en el repositorio de Share Point corresponde a GRNAGU_028_GuiaAnlisisdelImpactodelNegocio_v004_1 (3), el cual corresponde a la misma versión revisada en la vigencia 2022, en donde la OFCIN en el informe de auditoría 18 A de 2022 registró la OMC2 recomendando la importancia de la actualización de dicho documento ajustándolo a la realidad actual de la Entidad para estructurar y monitorear el PCN de Caja Honor; se aclara que el PMP suscrito para subsanar tal

debilidad, se encuentra vigente hasta el próximo 31-08-2023. Es de anotar que dicho documento es catalogado como confidencial y por tanto no es factible descargarlo del repositorio documental Isolucion.

Manual de Gestión de Plan de Continuidad del Negocio - PCN GR-NA-MA-008, V6 de 25-04-2023

La OFCIN al verificar el Manual de Gestión de Plan de Continuidad del Negocio - PCN GR-NA-MA-008, V6 de 25-04-2023, realiza la siguiente recomendación:

Recomendación 1.

La OFCIN recomienda a OAGRI incluir en la parte normativa del Manual del Gestión de Plan de Continuidad del Negocio - PCN la Norma ISO 27001:2013 Gestión de Seguridad de la Información Anexo A numeral 17. Aspectos de Seguridad de la Información de la Gestión de continuidad de Negocio, la Circular externa 029 de 2014 de la SFC. Asimismo, teniendo en cuenta que en los documentos controlados el control de cambios oficial es registrado en la herramienta Isolucion, la OFCIN recomienda realizar las gestiones pertinentes en coordinación con OAPLA para la actualización de dicho documento, eliminado la Tabla 1. Bitácora de Modificación puesto que en lo relativo a la versión 6, presenta fecha diferente a la fecha registrada en el repositorio Isolucion, así:

Tabla 1 Control de Cambios Manual de gestión de Plan de Continuidad del Negocio - PCN

Tabla *1*. Bitácora de Modificación

Bitácora de modificaciones			
No.	**Sección y No. de página modificada**	**Descripción del cambio**	**Fecha de modificación**
1	No aplica	Primera Versión del Documento	30/06/2017
2		Versión 2	16/08/2017
3		Versión 3	03/05/2019
4		Versión 4	23/01/2020
5	4,5,6	Versión 5	24/05/2022
6	7,8,11,13,14,15,16, 17,29	Versión 6	23/03/2023

Fuente: OAGRI - Repositorio SharePoint: OAGRICajaHonor - DOCUMENTACIÓN - Todos los documentos (sharepoint.com)

5.3.2. Revisión documentación suministrada por los procesos

OAGRI

Una vez consultado con OAGRI (Colaborador encargado del simulacro de continuidad y contingencia - Profesional Especializado 01 - Ing. de ciberseguridad y Plan de Continuidad de Negocio), indica que durante la vigencia 2023 no se ha efectuado simulacro de continuidad, agregando que se tiene planeado para el mes de junio de la presente vigencia realizar el primer simulacro involucrando servicios de página y portales web.

Así las cosas, teniendo en cuenta lo indicado por OAGRI y además que el ejercicio del simulacro realizado en la vigencia 2022, no contempló en su alcance la totalidad de los Puntos de Atención y servicios críticos de la Entidad, la OFCIN hace especial énfasis

NIT: 860021967 - 7
Centro de Contacto al Ciudadano CCC en Bogotá 601 755 7070
Línea gratuita nacional 01 8000 185 570
www.cajahonor.gov.co - contactenos@cajahonor.gov.co
Carrera 54 No. 26-54 - Bogotá D.C. Colombia
BIENESTAR Y EXCELENCIA

respecto a la **Oportunidad de Mejora Preventiva 01** registrada en el informe de Auditoría 18A de 2022, recomendando:

Recomendación 2.

La OFCIN recomienda a OAGRI en coordinación con OAINF, realizar por lo menos una prueba anual a las estrategias de Continuidad del Negocio definidas, acorde con las buenas prácticas de la Norma ISO 22301:2012 Capitulo 8 Operaciones; en el numeral 8.5 Ejercicios y pruebas, Norma ISO 27001:2013 Gestión de Seguridad de la Información Anexo A numeral 17. Aspectos de Seguridad de la Información de la Gestión de continuidad de Negocio, que involucre además de los servicios de página y portales web, la totalidad de Puntos de Atención y servicios críticos de la Entidad, verificando así el grado de preparación con que cuenta Caja Honor para la atención de eventos adversos que se puedan presentar y su recuperación en el menor tiempo posible minimizando la afectación del servicio y la posible materialización del R029 - Fallas en la Administración PCN entre otros, y la Dimensión 3°de MIPG V5 de 2023, Gestión con valores para el resultado.

Igualmente, se revisan los siguientes documentos que acorde a lo indicado por el Profesional Especializado 01 de OAGRI, se llevó a cabo mesas de trabajo con cada uno de los procesos tendiente a establecer los colaboradores claves que conforman el árbol de llamadas para el proceso de simulacros de continuidad y contingencia:

5.3.2.1. ARBOL DE LLAMADA

Para la vigencia 2023, se observa que la OAGRI ha llevado a cabo mesas de trabajo con los diferentes procesos de la Entidad tendientes al levantamiento de información para la construcción del árbol de llamadas que será utilizado en el momento del desarrollo del simulacro de continuidad y contingencia del negocio que se efectuará en la vigencia. Así las cosas, suministró la siguiente información:

Figura 6 OAGRI - Mesas de Trabajo – Procesos Caja Honor – Levantamiento inf Árbol de Llamadas
Fuente: Repositorio SharePoint: OAGRICajaHonor - ARBOL DE LLAMADA - Todos los documentos (sharepoint.com)

Área de Atención al Consumidor Financiero – ARACF

Se observa documento de fecha 20 de abril de 2023 correspondiente al Informe Activación Simulacro Árbol de Llamadas Área de Atención Consumidor Financiero (ARACF), en donde se especifica la siguiente composición del árbol de llamada para simulacro de continuidad y contingencia, logrando realizar el ejercicio en 10 minutos, con contestación de todos los incluidos en el árbol así:

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá ***601 755 7070***
Línea gratuita nacional ***01 8000 185 570***
www.cajahonor.gov.co - ***contactenos@cajahonor.gov.co***
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

Figura 7 Árbol de llamadas ARACF
Fuente: Repositorio SharePoint: OAGRICajaHonor - ARBOL DE LLAMADA - Todos los documentos (sharepoint.com)

ÁREA-OPERACIONES

Documento de fecha 20 abril de 2.023 correspondiente al **informe activación simulacro** árbol de llamadas Área de operaciones, el cual está compuesto por los siguientes colaboradores, los cuales durante el ejercicio fueron contactados con éxito:

Figura 8 Composición Árbol de Llamadas Área de Operaciones
Fuente: Repositorio SharePoint: OAGRICajaHonor - ARBOL DE LLAMADA - Todos los documentos (sharepoint.com)

No obstante, en la información antes citada no se evidencia el orden del flujo de llamadas a ejecutar en el proceso de simulacro de continuidad y contingencia, por lo que es importante tener total claridad al respecto para la consolidación del árbol de llamadas de la Entidad al momento de la ejecución del ejercicio de simulacro de continuidad y contingencia 2023.

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA
NIT: 860021967 - 7
Centro de Contacto al Ciudadano CCC en Bogotá ***601 755 7070***
Línea gratuita nacional ***01 8000 185 570***
www.cajahonor.gov.co *-* ***contactenos@cajahonor.gov.co***
Carrera 54 No. 26-54 - Bogotá D.C. Colombia
BIENESTAR Y EXCELENCIA

GERENCIA - GENERAL

Documento de fecha 14 de abril de 2023 correspondiente al **informe activación simul**acro árbol de llamadas Área Asuntos Gerenciales en donde se indica que los colaboradores que hacen parte del mismo son:

Figura 9 Composición Árbol de Llamadas Gerencia General
Fuente: Repositorio SharePoint: OAGRICajaHonor - ARBOL DE LLAMADA - Todos los documentos (sharepoint.com)

PABAR-PUNTO DE ATECCION BARRANQUILLA

Documento de fecha 21 de abril de 2023 correspondiente al informe activación simulacro árbol de llamadas Punto de Atención Barranquilla, cuyo objetivo es lograr comunicación inmediata con todos los funcionarios del Punto de Atención, indicando la relación de colaboradores contactados:

Tabla 2 Personal Árbol de Llamadas PABAR

Fuente: Repositorio SharePoint: OAGRICajaHonor - ARBOL DE LLAMADA - Todos los documentos(sharepoint.com)

No obstante, en la información antes citada no se evidencia el orden del flujo de llamadas a ejecutar en el proceso de simulacro de continuidad y contingencia, por lo que es importante tener total claridad al respecto para la consolidación del árbol de llamadas de la Entidad al momento de la ejecución del ejercicio de simulacro de continuidad y contingencia 2023.

PUNTO DE ATENCION

PABUC-Bucaramanga

Documento de fecha 24 de abril de 2023 correspondiente a Informe Activación Simulacro Árbol de Llamadas Punto de Atención PABUC, en donde se indica que El día 22 de abril

Fuente: Repositorio SharePoint: OAGRICajaHonor - ARBOL DE LLAMADA - Todos los documentos(sharepoint.com)

PAFLO

Documento de fecha 27 de abril de 2023, correspondiente a Informe Activación Simulacro

Tabla 4 Personal Árbol de Llamadas PAFLO

Fuente: Repositorio SharePoint: OAGRICajaHonor - ARBOL DE LLAMADA - Todos los documentos(sharepoint.com)

PAIBA

Documento de fecha 24 de abril de 2023, correspondiente a Informe Activación Simulacro Árbol de Llamadas Punto de Atención Ibagué, en donde se indica que el día 21 de abril

Tabla 5 Personal Árbol de Llamadas PAIBA

PAMED

Documento de fecha 02 de abril de 2023, correspondiente a Informe Activación Simulacro Árbol de Llamadas Punto de Atención Medellín, en donde se indica que el día 29 de abril de 2.023, se inició el simulacro de árbol de llamadas a partir de las 12:00 m. finalizando la

Tabla 6 Personal Árbol de Llamadas PAMED

UCODI-Unidad Control Disciplinario interno

Documento de fecha 20 de abril de 2023, correspondiente a Informe Activación Simulacro Árbol de Llamadas Unidad Control Disciplinario Interno, en donde se indica que el día 20 de abril de 2.023, inicié el simulacro de árbol de llamadas a partir de las 8:00 p.m.,

Acorde a lo anteriormente documentado, la OFCIN realiza la siguiente recomendación:

Recomendación 3.

La OFCIN recomienda a OAGRI que previo a la ejecución del simulacro de continuidad y contingencia 2023, se elabore, documente y socialice con todo el personal involucrado en el ejercicio, el árbol de llamadas descriptivo con los datos de los colaboradores que harán parte activa de dicho simulacro de Plan de continuidad del Negocio, registrando información relacionada con nombres y apellidos, cargo, número de contacto y rol que desempeña en el simulacro. Asimismo, probar el árbol de llamadas consolidado haciendo un recorrido en una sala de conferencias o en otra ubicación de la oficina, en tanto que este proceso garantiza que todos sepan qué hacer cuando se inicia el árbol de llamadas de emergencia, confirma que el procedimiento del árbol de llamadas funciona de acuerdo con el plan y valida que la información de contacto sea correcta. Lo anterior, en aras de

dar cumplimiento a las buenas prácticas para el desarrollo de simulacros del Plan de continuidad del Negocio descritos en la Norma ISO 22301 Sistemas de gestión de continuidad del negocio, además de MIPG V5 de 2023, Dimensiones 3 Gestión con Valores para Resultados y 5 Información y Comunicación, minimizando la materialización de riesgos asociados con R029 - Fallas en la Administración PCN y R102 - Fallas en Planes de Contingencia.

Ahora bien, una vez que se ha notificado todo el árbol de llamadas, se pueden continuar con otros procedimientos del plan de continuidad del negocio. Así las cosas, con el árbol de llamadas se obtienen beneficios que incluyen la interacción humana, la capacidad de transmitir información importante y la creación de una lista completa de información de contacto de los empleados.

Asimismo, para la vigencia 2023, la OAGRI suministró información relacionada con evidencias de la gestión realizada por el proceso frente a la planeación requerida para el ejercicio de simulacro de continuidad y contingencia que se tiene proyectado llevar a cabo en la vigencia actual, a continuación se presentan las comunicaciones remitidas a las partes interesadas:

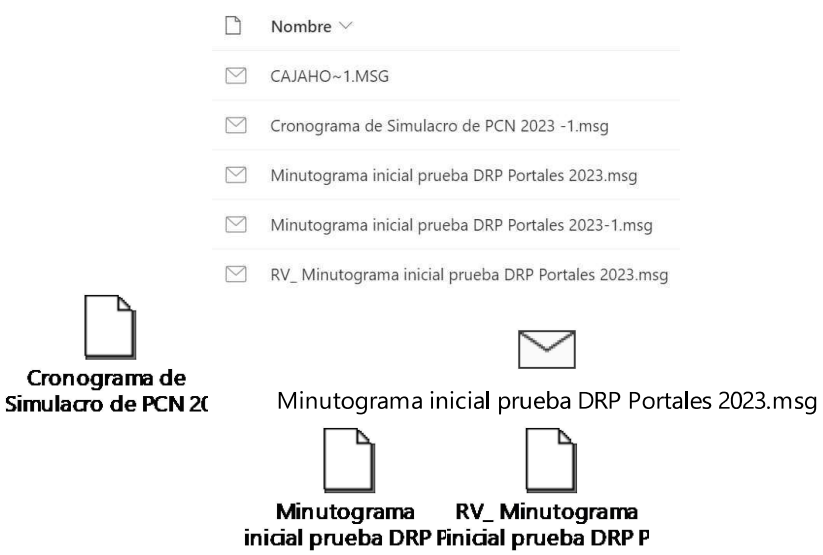

Figura 10 OAGRI Evidencias gestión para Simulacro 2023
Fuente: OAGRICajaHonor - SIMULACRO 2023 - Todos los documentos (sharepoint.com)

No obstante, teniendo en cuenta entrevista realizada con el Profesional Especializado 01 de OAGRI manifiesta que a la fecha 15-06-2023 no se tiene certeza de la fecha exacta en la cual se llevará a cabo el simulacro de contingencia y continuidad vigencia 2023.

Por otra parte, la OAGRI suministró información correspondiente a la prueba DRP simulacro de continuidad y contingencia desarrollado en la vigencia 2022, documentación elaborada por el proveedor Claro, la cual previamente fue analizada por la OFCIN en ejercicio de auditoría realizado en Diciembre de 2022 y documentado en informe de Auditoría 18 A:

Figura 11 Documentación Soporte Simulacro Continuidad y Contingencia 2022
Fuente: OAGRICajaHonor - SIMULACRO 2022-REALIZADO - Todos los documentos (sharepoint.com)

Archivo_Control_App

Describe si hubo conexión a las aplicaciones en los diferentes puntos de atención de Caja Honor:

Figura 12 Archivo Control App – Pruebas DRP Control de Acceso a Aplicaciones Puntos de Atención
Fuente: OAGRICajaHonor - INFORME CLARO - Todos los documentos (sharepoint.com)

Copia de Árbol de llamadas -DRP-PCN- 2022 Actualizado-auditoria

Contiene el DIRECTORIO PERSONAL - DRP CAJA HONOR / RIESGOS de los Procesos Funcionales, OAINF y CLARO, en donde el detalle de la información se puede observar en el siguiente archivo:

Detalle_RTO_PruebaDRP_26Ago2022

Contiene el Minutograma ejecución de actividades Prueba DRP Caja Honor 26 y 27 Agosto 2022 Detalle R.T.O., como se muestra a continuación:

NIT: 860021967 - 7
Centro de Contacto al Ciudadano CCC en Bogotá 601 755 7070
Línea gratuita nacional 01 8000 185 570
www.cajahonor.gov.co - contactenos@cajahonor.gov.co
Carrera 54 No. 26-54 - Bogotá D.C. Colombia
BIENESTAR Y EXCELENCIA

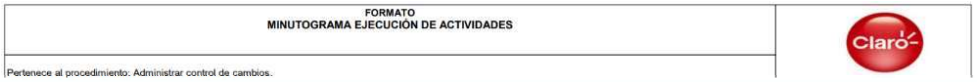

Figura 13 Minutograma ejecución de actividades Prueba DRP Caja Honor 26 y 27 Agosto 2022 Detalle R.T.O
Fuente: OAGRICajaHonor - INFORME CLARO - Todos los documentos (sharepoint.com)

Hitos de control_PruebaDRP_26 y 27Agosto 2022

Contiene el Formato Hitos de Control Prueba DRP 26 y 27 Agosto 2022 DRP Caja Honor – Claro, información que se puede observar a detalle en el siguiente archivo:

Hitos de control_PruebaDRP_

Informe Técnico ejercicio DRP Caja Honor_20220826

Contiene Prueba técnica DRP - Caja Honor ejecutada con fecha 26 – 27 agosto 2022, mayor detalle se puede observar en el siguiente archivo:

Informe Técnico ejercicio DRP Caja H

Matriz_Riesgos_Prueba_DRP_26 y 27 agosto2022

Contiene el Análisis de Riesgos Prueba DRP desarrollada los días 26 y 27 agosto 2022, mayor detalle se puede observar en el siguiente archivo:

Matriz_Riesgos_Prueba_DRP_26y27 ago

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá ***601 755 7070***
Línea gratuita nacional ***01 8000 185 570***
www.cajahonor.gov.co *-* ***contactenos@cajahonor.gov.co***
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

Por otra parte, la OFCIN verificó en la herramienta Isolucion los Riesgos y Puntos de Control asociados al proceso OAGRI, como se puede observar en la siguiente imagen:

RIESGO	CAUSA	CONTROL
R005 - FALLAS EN LOS SISTEMAS DE INFORMACION	CA007 - FALLAS Y ERRORES EN LOS SISTEMAS DE INFORMACIÓN	CO030 - SOPORTE Y MANTENIMIENTO CON PROVEEDORES
		CO044 - PRUEBAS PLAN DE CONTINUIDAD DEL NEGOCIO
R010 - INCUMPLIMIENTO DE OBLIGACIONES LEGALES Y/O NORMATIVAS APLICABLES A LA ENTIDAD	CA010 - FALTA DE ACTUALIZACIÓN DE LOS PROCEDIMIENTOS, INCUMPLIMIENTO DE LA NORMATIVA	CO015 - CUMPLIMIENTO DE LOS PROCEDIMIENTOS DEL PROCESO
		CO036 - CONSULTA NORMATIVIDAD SFC
		CO211 - CAPACITACION EN LOS SISTEMAS DE GESTION DEL RIESGO
	CA118 - FALLAS EN LAS POLITICAS DE CONOCIMIENTO DEL CLIENTE	CO179 - BLOQUEO DE MATRICULA INMOBILIARIA EN EL SISTEMA DE INFORMACION INTERNO
		CO180 - BLOQUEO DE BENEFICIARIO DE GIRO, VENDEDOR DEL INMUEBLE O TERCERO RECEPTOR DEL GIRO
		CO181 - BLOQUEO BENEFICIARIO DE GIRO INSTITUCIONES EDUCATIVAS
	CA138 - FALLAS EN LOS CANALES DE COMUNICACIÓN	ca124 - CANAL ALTERNO DE COMUNICACIÓN
		ca125 - USO DE MODEM EXTERNO
	CA148 - SUMINISTRAR A LOS CONSUMIDORES FINANCIEROS INFORMACIÓN VERBAL O ESCRITA QUE NO CUMPLA CON CRITERIOS DE OPORTUNIDAD Y CALIDAD.	CO214 - REALIZAR EL RESPECTIVO CONTROL DE CALIDAD A LAS RESPUESTAS DE LAS SOLICITUDES DE LOS CONSUMIDORES FINANCIEROS Y DEMÉS PARTES INTERESADAS QUE SEAN RESPONSABILIDAD DEL PROCESO
R023 - FALLAS EN EL REPORTE Y DOCUMENTACION DE LOS RIESGOS	CA023 - DEBILIDADES EN LA GENERACIÓN DE INFORMACIÓN Y ADOPCIÓN DE METODOLOGÍAS PARA GESTIONAR LOS SAR	CO012 - VERIFICACION DE LA INFORMACION DEL AREA
		CO025 - PLAN DE CAPACITACION
R029 - FALLAS EN LA ADMINISTRACION PCN	CA029 - FALTA DE ACTUALIZACIÓN Y CAPACITACION DE LOS PROCEDIMIENTOS FRENTE A LA NORMATIVIDAD	CO044 - PRUEBAS PLAN DE CONTINUIDAD DEL NEGOCIO
		CO102 - SEGUIMIENTO A LAS DEFICIENCIAS DE PCN
RSI031 - PERDIDA DE INFORMACION	CSI023 - FALTA DE COPIAS DE RESPALDO	KSI006 - COPIAS DE SEGURIDAD DE LA INFORMACIÓN (BACKUPS)
R035 - DEFICIENCIA EN LA CALIDAD Y ENTREGA INOPORTUNA DE LA	CA032 - INCONSISTENCIAS, ERRORES O MALA CALIDAD EN LA INFORMACION RECOLECTADA EN LOS SISTEMAS DE INFORMACION O REMITIDA POR LOS PROCESOS.	CO022 - VALIDACIÓN DE INFORMACIÓN
		CO099 - SEGUIMIENTO A LAS ACTIVIDADES PROGRAMADAS
R074 - INCUMPLIMIENTO DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD	CA074 - DEFICIENCIAS EN LAS HERRAMIENTAS DE CIBERSEGURIDAD	CO023 - ACUERDO DE CONFIDENCIALIDAD
		CO031 - POLITICAS DE BACKUP
		CO053 - CLAUSULAS CONTRACTUALES
		CO091 - SEGUIMIENTO A LA INFRAESTRUCTURA TECNOLÓGICA DE LA ENTIDAD
R091 - FALLAS EN LA GESTION Y ADMINISTRACION DEL DATA CENTER CAN	CA100 - FALTA DE SEGUIMIENTO A LA GESTION TECNICA REALIZADA AL DATA CENTER ALTERNO - CAN	CO145 - SEGUIMIENTO AL INFORME DIARIO DE ALMACENAMIENTO DE LA 3PAR
		CO147 - CONTRATACIÓN DE MANOS EXPERTAS
R102 - FALLAS EN PLANES DE CONTINGENCIA	CA122 - FALTA DE CONOCIMIENTO DE LOS PLANES DE EMERGENCIAS, CONTINGENCIAS Y CONTINUIDAD DE NEGOCIO DE CAJA HONOR POR PARTE DE LOS FUNCIONARIOS.	CO142 - APLICAR EL PLAN DE CONTINGENCIA DEL PROCESO
		CO183 - SOCIALIZAR LOS DOCUMENTOS DEL PLAN DE CONTINGENCIA

Figura 14 Matriz de riesgos relacionados a PCN, con sus causas y controles asociados.
Fuente: http://vigia:8080/WebSvc/riesgocontroles.php?0=proes.gr
Consultado: 20-06-2023

Minutograma_Caja_Honor_PruebaDRP_26Agosto2022_rev26082022

Contiene el Minutograma Ejecución de Actividades Prueba DRP TOTAL Caja Honor realizado los días 26 y 27 agosto 2022, documento elaborado por el proveedor Claro, mayor detalle se puede observar en el siguiente archivo:

Minutograma_Caja Honor_PruebaDRP_

5.3.2.2. Presupuesto PCN

Figura 15 Presupuesto asignada para PCN
Fuente: Herramienta SEVEN – Consultado 14-06-2023

5.3.2.3. Punto Alterno PAC

Guía de Usuario Punto Alterno – PAC

La OFCIN realizó verificación del documento GR-NA-GU-005 V11 de 13-02-2023 Guía del usuario Punto Alterno de Continuidad_PAC, el cual debe ser objeto de actualización ajustándolo a la actual situación de Caja Honor, en donde se está llevando a cabo en su gran mayoría trabajo presencial y entre otros, actualizar la información relacionada con las líneas telefónicas registradas en dicho documento ya que no corresponden a las vigentes.

Figura 16 Registro Fotográfico Centro Alterno de Continuidad – PABUC
Fuente: Líder PABUC – Registro Fotográfico enviado vía Chat WhatsApp – 20-06-2023

Agregando además, que dichos equipos de cómputo no se utilizan desde la época de la pandemia, no teniéndose a la fecha determinación oficial respecto a la destinación de

éstos, observándose subutilización de equipos tecnológicos lo que impacta de manera negativa los activos y patrimonio de la Entidad.

Igualmente, la OFCIN requirió al líder de PABUC el inventario de equipos de cómputo asignados para el PCN, para lo cual el Punto de Atención suministró el archivo denominado INV. PCN.pdf del cual se filtraron los ítems relacionados con equipos de cómputo (De escritorio y Portátiles) en un total de 25 máquinas:

Con la anterior información, la OFCIN procedió a realizar el cruce por número de placa con el inventario de equipos de cómputo que registra en ALMAC, evidenciando la coincidencia de la información en la cantidad de equipos, los cuales se encuentran a

Fuente: OAINF Email del 23-06-2023

Oportunidad de Mejora Correctiva 1:

En cumplimiento a lo expuesto en el numeral 5.3.2.3 del presente informe, lo cual fue evidenciado por la OFCIN durante la ejecución del ejercicio auditor, es prioritario que OAINF en coordinación con OAGRI y ALMAC lleven a cabo la gestión pertinente para establecer el destino de los 25 equipos de cómputo que en principio fueron asignados para la operación del Punto Alterno de Continuidad ubicado en PABUC y que desde hace aproximadamente 2 años no se encuentran operando, por lo que es prioritario determinar su funcionamiento y cumplimiento de las tareas específicas para las cuales fueron implementados y su disposición, en donde es necesaria la actuación de la OAINF aportando el concepto técnico pertinente a efectos de determinar el proceder de los mismos, ya sea para ser reasignados a otro proceso o para dar de baja a dichas máquinas según corresponda. En caso de que la determinación sea dar de baja siempre y cuando aplique la Resolución de baja, ejecutar la gestión pertinente a dicho proceso en el menor tiempo posible; en aras de dar cumplimiento a las buenas Prácticas de Seguridad de la información y Ciberseguridad emanadas de la ISO NTC 27001:2013 en su Anexo A, Numeral A.8, Gestión de Activos, A.11. Seguridad Física y del Entorno, A.12. Seguridad de las Operaciones, A.16. Gestión de Incidentes de Seguridad de la Información, A.17. Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio, Manual para el Manejo de Bienes Muebles e Inmuebles AS-NA-MA-001 versión 6 del 20-sep-2022, Manual de Seguridad de la Información y Ciberseguridad GR-NA-MA-009 versión 3 aprobada el 25-06-2021, Resolución 7870 del 2022 “Política General de Seguridad y Privacidad de la Información para el Sector Defensa” MDN, con el fin de minimizar la materialización del RSI029 - Perdida de la integridad del activo de información, R052 - Fallas en la Administración del Inventario, R054 - Fallas en la administración de bienes muebles e inmuebles, R074 - Incumplimiento de las políticas de seguridad de la información y ciberseguridad, RSI031 - Pérdida de Información, RO10 Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad, R068 - Insuficiencia; Obsolescencia y/o Subutilización de los Activos Tecnológicos a fin de fortalecer el autocontrol como principio rector del Sistema de Control Interno en los procesos y dar cumplimiento de las Dimensiones de MIPG 5° Información y Comunicación y 7° Control Interno en sus componentes Actividades de Control y Actividades de Monitoreo.

5.3.2.4. VPN IMPLEMENTADAS CAJA HONOR

Tabla 7 Lista VPN Grupo vpn´s-IT-SOPORTE

ACTIVO a corte del 23-06-2023, con el siguiente detalle:

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá ***601 755 7070***
Línea gratuita nacional ***01 8000 185 570***
www.cajahonor.gov.co *-* ***contactenos@cajahonor.gov.co***
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

Fuente OAINF Archivo Copia de Grupos VPN.xlsx, Libro CORRERIAS CORTE 23 JUNIO

Igualmente, en prueba de recorrido realizada el 26-06-2023 con el profesional Universitario 04 de OAINF, se indagó respecto a la herramienta tecnológica implementada en la Entidad para el manejo de las VPN, quien indicó que se utiliza la plataforma de colaboración empresarial Check Point, así:

Por otra parte, se indicó que en la herramienta check Point se cuenta con el Módulo Mobile Acces mediante el cual se permite generar el log de eventos de conexión a la VPN por usuario específico, para lo cual se procedió a tomar una muestra de éste, generando reporte general y detallado, así:

Figura 22 OAINF pantalla log de eventos de conexón a VPN – Detalle - 26 de junio de 2023
Fuente Correo Electrónico OAINF 26-06-2023.

Adicionalmente, se indicó por parte del profesional Líder de Mesa de Ayuda, que la Entidad cuenta con un robot implementado, mediante el cual se genera de manera semiautomática (requiere intervención humana) el envío de alertas en los casos de vencimiento de la fecha de término de accesos al servicio de VPN, para lo cual se suministró evidencias mediante email de OAINF – Mesa de Ayuda de fecha 26-06-2023, tal como se muestra en la figura 22:

De la misma forma, la OFCIN con el fin de contar con mayor información referente al Robot implementado para el envío de alertas proceso de gestión VPN, requirió a OAINF el suministro de información detallada en relación al tema y la documentación de dicho proceso; para lo cual la OAINF con fecha 28-06-2023 remitió vía Teams video explicando el proceso, en donde se indica que se trata del "BOT Notificador de VPN" el cual se ejecuta en 3 procesos:

1. Abrir archivos Excel
2. Revisar VPN vencidas y enviar correo electrónico
3. Revisar VPN próximas a vencer

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá ***601 755 7070***
Línea gratuita nacional ***01 8000 185 570***
www.cajahonor.gov.co *-* ***contactenos@cajahonor.gov.co***
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

Así las cosas, el TECNICO 01 de la OAINF ejecuta el Bot mediante la herramienta UiPath, que permite configurar robots para procesos específicos y corresponde a la interfaz con la que el usuario interacciona con el robot; de aquí en adelante el Bot hace solo las tareas correspondientes y deja log mostrando cada una de las actividades que va realizando, así:

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá ***601 755 7070***
Línea gratuita nacional ***01 8000 185 570***
www.cajahonor.gov.co *-* ***contactenos@cajahonor.gov.co***
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

3. Abre plantilla envió correo electrónico y pega la tabla resultados de los filtros:

4. Da click en enviar correo electrónico y remite la información al personal responsable de desactivación de las VPN.
5. Ejecuta el mismo proceso para las VPN próximas a vencer:

Como se observa en las figuras 25 Alertas Formatos VPN Vencidos – 26-06-2023, 26 Filtro realizado por Bot, VPN Vencidas y 27 Resultado VPN Vencidas realizado por Bot, plantilla Correo Electrónico, la OFCIN evidencia que no se efectúa una adecuada y oportuna gestión de las VPN implementadas, dado que acorde a los reportes generados por el RPA (Robotic process automation), al 26-06-2023 y al 27-06-2023 presentados en el video Explicación – Bot Notificador VPN suministrado por OAINF, existen VPN en donde los permisos de acceso no han sido desactivados, siendo que los mismos vencieron desde el 08, 09 y 10 de junio de la presente vigencia respectivamente. Por otra parte, es de vital importancia la documentación y socialización al interior de OAINF, de los diferentes procesos implementados, puesto que la OFCIN pudo evidenciar que los colaboradores entrevistados en las pruebas de recorrido no tenían conocimiento respecto del Robot (RPA) implementado para el reporte de alertas relacionadas con el vencimiento de accesos al servicio de VPN.

No obstante, el Bot Notificador VPN, el Módulo de Móvil Acess de Check Point, implementado en la Entidad, que apoyan en parte el proceso de gestión de VPN, es importante la implementación de una herramienta tecnológica que permita realizar una gestión eficaz de los usuarios con VPN, facilitando el monitoreo de todos los equipos de la red, además de que se registre la trazabilidad correspondiente a eventos de conectividad del usuario y así contar con información documentada, actualizada y oportuna y se tenga la posibilidad de generar reportes del proceso.

5.3.2.5. Infraestructura Data Center Alterno

La OAINF mediante el archivo Infraestructura Datacenter Alterno – CAN.ppt suministró información relacionada con la Topología General Caja Honor, tanto para el CDP como

Fuente: OAINF – Archivo archivo Infraestructura Datacenter Alterno – CAN.ppt

Así mismo, se observan los elementos de Infraestructura, Ciberseguridad y Comunicaciones con los que cuenta la Entidad, para así:

Fuente ARTAH Email 26-06-2023

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá ***601 755 7070***
Línea gratuita nacional ***01 8000 185 570***
www.cajahonor.gov.co *-* ***contactenos@cajahonor.gov.co***
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

Al consultar con Mesa de Ayuda frente a si todos los colaboradores autorizados para trabajo en casa cuentan con VPN implementada, el profesional Universitario 03 Coordinador Mesa de Ayuda - Oficina Asesora de Informática indica que "Pueden estar autorizados por talento humano en caso que se requiera pero no quiere decir que tengan el formato o instalada la VPN".

Así las cosas, se requirió el suministro del formato de GR-NA-FM-020 Formato Acuerdo de Confidencialidad para Uso de Dispositivos Móviles y Acceso Remoto debidamente diligenciado para cada uno de los colaboradores reportados por ARTAH con permiso de trabajo en casa, además de la complementación de la información correspondiente a datos relacionados con el proceso o dependencia en la que prestan sus servicios, Fecha de Inicio, Fecha de Término y Estado, para lo cual OAINF – Mesa de Ayuda suministró la siguiente información:

Tabla 10 Listado de Colaboradores Caja Honor Autorizados Trabajo en Casa
Información complementada por OAINF

diligenciado, Fuente OAINF Email 29-06-2023

Sin embargo, en prueba de recorrido llevada a cabo con Mesa de Ayuda con fecha 12-07-2023, se solicita realizar la consulta
donde se observa que dicho usuario se

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá ***601 755 7070***
Línea gratuita nacional ***01 8000 185 570***
www.cajahonor.gov.co *-* ***contactenos@cajahonor.gov.co***
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

Dado lo anterior y teniendo en cuenta que para la implementación y activación del servicio de VPN es requisito el diligenciamiento del formato GR-NA-FM-020 Formato Acuerdo de Confidencialidad para Uso de Dispositivos Móviles y Acceso Remoto es prioritario la consecución y conservación de dicho formato para el usuario

Igualmente, en la tabla 10 se observa la existencia de personal que terminó su periodo de trabajo en casa en la vigencia 2022 y primer trimestre de 2023 y aún son reportados por ARTAH en el listado de personal con trabajo en casa, por lo que es importante la actualización de dicha información:

Por otra parte, no se observa coincidencia de la información del personal con autorización para trabajo en casa reportado por ARTAH y las VPN implementadas, puesto que dentro del listado de VPN reportadas por OAINF no se contempla la totalidad de colaboradores reportados por ARTAH, con trabajo en casa.

Dado lo anteriormente expuesto la OFCIN realiza la siguiente recomendación:

Oportunidad de Mejora Correctiva 2.

La OFCIN recomienda a OAINF en coordinación con ARTAH, realizar la depuración de la información correspondiente al Personal con Autorización de Trabajo en Casa y con VPN

implementada para conexión de red privada para el desarrollo de sus actividades, además de mantener documentada, actualizada y completa la información correspondiente a los formatos de autorización debidamente diligenciados. Igualmente, se recomienda estudiar la posibilidad de automatización del proceso para la gestión y control eficaz de VPN con el registro de toda la información pertinente (nombre del colaborador, cargo, dependencia, fecha de implementación, fecha de termino, entre otros), facilitando el monitoreo de todos los equipos de la red y estableciendo control en los accesos, es decir asegurando el acceso de los usuarios autorizados y evitar el acceso no autorizado a los servicios de VPN, conservando la trazabilidad transaccional aplicada a cada usuario (eventos de conectividad, etc.), en lo posible gestionando en forma digital el formato de autorización como por ejemplo la implementación de un flujo en el gestor documental Dodo Docs, en donde se registran con rubrica o digitalmente la firma del personal involucrado en el proceso, y además contar con la posibilidad de generación de reportes automáticos de un periodo de tiempo dado. Lo anterior, tendiente a eliminar procesos manuales que conllevan a mayor margen de error e indisponibilidad de la información, la cual debe en todo momento ser precisa, confiable y oportuna para los procesos que la requieran, minimizando el desgaste administrativo en la búsqueda de los formatos físicos y así preservar los pilares fundamentales de la seguridad de la información como son confidencialidad, integridad y disponibilidad descritos en ISO 27001:2013, dando cumplimiento a las Políticas de Seguridad de la Información y Ciberseguridad descritas en el GR-NA-MA-009 Manual de Seguridad de la Información y Ciberseguridad versión 3 aprobada el 25-06-2021, Resolución 7870 del 2022 “Política General de Seguridad y Privacidad de la Información para el Sector Defensa” MDN, y en aras de minimizar la materialización de riesgos asociados con RSI029 - Pérdida de la integridad del activo de información, RSI005 - Pérdida de la Disponibilidad del Activo de Información, RSI067 - Fuga de Información, RSI031 - Pérdida de Información, RSI030 - Información Errada, R010 - Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad; con el propósito de fortalecer el autocontrol como principio rector del Sistema de Control Interno en los procesos y dar cumplimiento de las Dimensiones de MIPG V5 de marzo 2023 dimensiones 3ª Gestión con Valores para Resultado y 5ª Información y comunicación.

5.3.2.7. Registro de eventos de riesgo ocurridos durante el periodo objeto de la presente auditoría y documentados en VIGIA.

La OAGRI suministró los archivos RERO 2022 Y ITRIM_2023.xlsx el cual contiene el registro de REROS distribuidos por trimestre correspondiente a las vigencias 2022 y I Trimestre 2023, así:

Fuente OAGRI Archivo RERO 2022 Y ITRIM_2023 – Libro II TRIM 2022.xlsx

Archivo RERO 2022 Y ITRIM_2023 – Libro III TRIM 2022:
Contiene un total de 17 registros distribuidos de la siguiente manera:

Tabla 12 Lista REROS III TRIM 2022

Fuente OAGRI Archivo RERO 2022 Y ITRIM_2023 – Libro III TRIM 2022.xlsx

Archivo RERO 2022 Y ITRIM_2023 – Libro IV TRIM 2022:
Contiene un total de 30 registros distribuidos de la siguiente manera:

Tabla 13 Lista REROS IV TRIM 2022

Fuente OAGRI Archivo RERO 2022 Y ITRIM_2023 – Libro IV TRIM 2022.xlsx

Archivo RERO 2022 Y ITRIM 2023 – Libro I TRIM 2023:
Contiene un total de 31 registros distribuidos de la siguiente manera:

Tabla 14 Lista REROS I TRIM 2023

Fuente OAGRI Archivo RERO 2022 Y ITRIM_2023 – Libro I TRIM 2023.xlsx

No obstante, que se evidencia reporte de REROS por parte de los diferentes procesos de la Entidad, no se observa que el perfil "Auditor" asignado a la OFCIN en la herramienta VIGÍA RERO, cuente con opción de consulta que permita verificar el seguimiento y acciones aplicadas para resolver cada uno de los REROS registrados en la plataforma, verificando su trazabilidad, tiempos de resolución, responsables, afectación, entre otros.

Así las cosas, la OFCIN recomienda:

Recomendación 4.

La OFCIN recomienda a OAGRI en coordinación con el proveedor de la herramienta VIGIA RERO, revisar y analizar la posibilidad de construir y unificar en el perfil de Auditor, la funcionalidad de consulta a todas las bondades de la aplicación como una opción de mejora a dicho software y de esta manera no limitar el desarrollo del ejercicio auditor. Igualmente, que se implemente el reporte automático de REROS que permita generación de éstos por periodos determinados, incluyendo datos de la especificación de los REROS y de las tareas llevadas a cabo para su resolución y demás trazabilidad. Lo anterior, con el objeto de permitir a la OFCIN la realización autónoma de las consultas, toma de evidencias y generación de reportes de información que considere pertinentes en la herramienta para el análisis de la información y documentación del informe de auditoría correspondiente.

NIT: 860021967 - 7
Centro de Contacto al Ciudadano CCC en Bogotá 601 755 7070
Línea gratuita nacional 01 8000 185 570
www.cajahonor.gov.co - contactenos@cajahonor.gov.co
Carrera 54 No. 26-54 - Bogotá D.C. Colombia
BIENESTAR Y EXCELENCIA

Conclusiones

La OFCIN identifica que la Entidad cuenta con documentación pertinente con relación al Plan de Continuidad del Negocio, tales como Manuales, Planes y Guías, no obstante, es importante aclarar que los mismos deben ser objeto de actualización, tal como se recomendó en el anterior ejercicio auditor mediante el Informe de Auditoría No. 18 A de 2022; para lo cual la OFCIN cargó en la herramienta SVE el PMP correspondiente, en el cual la OAGRI ha definidos las actividades a desarrollar para la subsanación de las vulnerabilidades encontradas, tareas que tienen fecha máxima de cumplimiento el próximo 31-08-2023.

En la vigencia 2023, no se han llevado a cabo pruebas o simulacros de Continuidad del Negocio que permitan verificar el grado de preparación en que se encuentra Caja Honor para afrontar la recuperación después de que un evento adverso haya ocurrido, evitando cualquier impacto significativo en la imagen y la reputación de la Entidad y garantizando al mismo tiempo la continuidad del negocio; además de dar cumplimiento en la administración del Plan de Continuidad del Negocio (PCN) acorde con lo requerido por la SFC en el Capítulo XXIII en la CBCF (CE 100 de 1995), las modificaciones realizadas a través de la CE 025 de 2020, numeral 3.1.3.2, las demás modificaciones y/o actualizaciones pertinentes.

Es de alta prioridad la definición del destino final de la infraestructura física que en su momento fue implementada en el Punto de Alterno de Continuidad en PABUC, la cual desde hace aproximadamente 2 años se encuentra inactiva. Lo anterior, con el fin de evitar posible detrimento patrimonial por subutilización o utilización inadecuada de equipos tecnológicos.

Con el fin de mantener un mayor control respecto a la gestión de las VPN implementadas en la Entidad, es importante el establecimiento de procesos automáticos que faciliten la tarea y guarden la trazabilidad pertinente a cada caso, aplicar la política de cero papel digitalizando los formatos de autorización respectiva, además de reducir los procesos manuales que incrementan el margen de error.

Concluida la Auditoría la OFCIN, generó 2 Oportunidades de Mejora y 4 Recomendaciones para la Oficina Asesora de Gestión del Riesgo y Áreas de trabajo interrelacionadas; de esta forma su seguimiento, se realizará en la próxima auditoría al Plan de Continuidad del Negocio.

Tabla de Recomendaciones y Oportunidades de Mejora

No.	OPORTUNIDADES DE MEJORA
1	**Oportunidad de Mejora Correctiva 1:** En cumplimiento a lo expuesto en el numeral 5.3.2.3 del presente informe, lo cual fue evidenciado por la OFCIN durante la ejecución del ejercicio auditor, es prioritario que OAINF en coordinación con OAGRI y ALMAC lleven a cabo la gestión pertinente para establecer el destino de los 25 equipos de cómputo que en principio fueron asignados para la operación del Punto Alterno de Continuidad ubicado en PABUC y que desde hace aproximadamente 2 años no se encuentran operando, por lo que es prioritario determinar su funcionamiento y cumplimiento

No.	OPORTUNIDADES DE MEJORA
	de las tareas específicas para las cuales fueron implementados y su disposición, en donde es necesaria la actuación de la OAINF aportando el concepto técnico pertinente a efectos de determinar el proceder de los mismos, ya sea para ser reasignados a otro proceso o para dar de baja a dichas máquinas según corresponda. En caso de que la determinación sea dar de baja siempre y cuando aplique la Resolución de baja, ejecutar la gestión pertinente a dicho proceso en el menor tiempo posible; en aras de dar cumplimiento a las buenas Prácticas de Seguridad de la información y Ciberseguridad emanadas de la ISO NTC 27001:2013 en su Anexo A, Numeral A.8, Gestión de Activos, A.11. Seguridad Física y del Entorno, A.12. Seguridad de las Operaciones, A.16. Gestión de Incidentes de Seguridad de la Información, A.17. Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio, Manual para el Manejo de Bienes Muebles e Inmuebles AS-NA-MA-001 versión 6 del 20-sep-2022, Manual de Seguridad de la Información y Ciberseguridad GR-NA-MA-009 versión 3 aprobada el 25-06-2021, Resolución 7870 del 2022 "Política General de Seguridad y Privacidad de la Información para el Sector Defensa" MDN, con el fin de minimizar la materialización del RSI029 - Perdida de la integridad del activo de información, R052 - Fallas en la Administración del Inventario, R054 - Fallas en la administración de bienes muebles e inmuebles, R074 - Incumplimiento de las políticas de seguridad de la información y ciberseguridad, RSI031 - Pérdida de Información, RO10 Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad, R068 - Insuficiencia; Obsolescencia y/o Subutilización de los Activos Tecnológicos a fin de fortalecer el autocontrol como principio rector del Sistema de Control Interno en los procesos y dar cumplimiento de las Dimensiones de MIPG 5° Información y Comunicación y 7° Control Interno en sus componentes Actividades de Control y Actividades de Monitoreo.
2	**Oportunidad de Mejora Correctiva 2.** La OFCIN recomienda a OAINF en coordinación con ARTAH, realizar la depuración de la información correspondiente al Personal con Autorización de Trabajo en Casa y con VPN implementada para conexión de red privada para el desarrollo de sus actividades, además de mantener documentada, actualizada y completa la información correspondiente a los formatos de autorización debidamente diligenciados. Igualmente, se recomienda estudiar la posibilidad de automatización del proceso para la gestión y control eficaz de VPN con el registro de toda la información pertinente (nombre del colaborador, cargo, dependencia, fecha de implementación, fecha de termino, entre otros), facilitando el monitoreo de todos los equipos de la red y estableciendo control en los accesos, es decir asegurando el acceso de los usuarios autorizados y evitar el acceso no autorizado a los servicios de VPN, conservando la trazabilidad transaccional aplicada a cada usuario (eventos de conectividad, etc.), en lo posible gestionando en forma digital el formato de autorización como por ejemplo la implementación de un flujo en el gestor documental Dodo Docs, en donde se registran con rubrica o digitalmente la firma del personal involucrado en el proceso, y además contar con la posibilidad de generación de reportes automáticos de un periodo de tiempo dado. Lo anterior, tendiente a eliminar procesos manuales que conllevan a mayor margen de error e indisponibilidad de la información, la cual debe en todo momento ser precisa, confiable y oportuna para los procesos que la requieran, minimizando el desgaste administrativo en la búsqueda de los formatos físicos y así preservar los pilares fundamentales de la seguridad de la información como son confidencialidad, integridad y disponibilidad descritos en ISO 27001:2013,

No.	OPORTUNIDADES DE MEJORA
	dando cumplimiento a las Políticas de Seguridad de la Información y Ciberseguridad descritas en el GR-NA-MA-009 Manual de Seguridad de la Información y Ciberseguridad versión 3 aprobada el 25-06-2021, Resolución 7870 del 2022 "Política General de Seguridad y Privacidad de la Información para el Sector Defensa" MDN, y en aras de minimizar la materialización de riesgos asociados con RSI029 - Perdida de la integridad del activo de información, RSI005 - Perdida de la Disponibilidad del Activo de Información, RSI067 - Fuga de Información, RSI031 - Perdida de Información, RSI030 - Información Errada, R010 - Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad; con el propósito de fortalecer el autocontrol como principio rector del Sistema de Control Interno en los procesos y dar cumplimiento de las Dimensiones de MIPG V5 de marzo 2023 dimensiones 3ª Gestión con Valores para Resultado y 5ª Información y comunicación.

No.	RECOMENDACIÓN
1	**Recomendación 1.** La OFCIN recomienda a OAGRI incluir en la parte normativa del Manual del Gestión de Plan de Continuidad del Negocio - PCN la Norma ISO 27001:2013 Gestión de Seguridad de la Información Anexo A numeral 17. Aspectos de Seguridad de la Información de la Gestión de continuidad de Negocio, la Circular externa 029 de 2014 de la SFC. Asimismo, teniendo en cuenta que en los documentos controlados el control de cambios oficial es registrado en la herramienta Isolucion, la OFCIN recomienda realizar las gestiones pertinentes en coordinación con OAPLA para la actualización de dicho documento, eliminado la Tabla 1. Bitácora de Modificación puesto que en lo relativo a la versión 6, presenta fecha diferente a la fecha registrada en el repositorio Isolucion.
2	**Recomendación 2**. La OFCIN recomienda a OAGRI en coordinación con OAINF, realizar por lo menos una prueba anual a las estrategias de Continuidad del Negocio definidas, acorde con las buenas prácticas de la Norma ISO 22301:2012 Capitulo 8 Operaciones; en el numeral 8.5 Ejercicios y pruebas, Norma ISO 27001:2013 Gestión de Seguridad de la Información Anexo A numeral 17. Aspectos de Seguridad de la Información de la Gestión de continuidad de Negocio, que involucre además de los servicios de página y portales web, la totalidad de Puntos de Atención y servicios críticos de la Entidad, verificando así el grado de preparación con que cuenta Caja Honor para la atención de eventos adversos que se puedan presentar y su recuperación en el menor tiempo posible minimizando la afectación del servicio y la posible materialización del R029 - Fallas en la Administración PCN entre otros, y la Dimensión 3°de MIPG V5 de 2023, Gestión con valores para el resultado.
3	**Recomendación 3.** La OFCIN recomienda a OAGRI que previo a la ejecución del simulacro de continuidad y contingencia 2023, se elabore, documente y socialice con todo el personal involucrado en el ejercicio, el árbol de llamadas descriptivo con los datos de los colaboradores que harán parte activa de dicho simulacro de Plan de continuidad del Negocio, registrando información relacionada con nombres y apellidos, cargo, número de contacto y rol que desempeña en el simulacro. Asimismo, probar el árbol de llamadas consolidado haciendo un recorrido en una sala de conferencias o en otra ubicación de la oficina, en tanto que este proceso garantiza que todos sepan qué hacer cuando se inicia el árbol de llamadas de emergencia, confirma que el procedimiento del árbol de llamadas funciona de

No.	RECOMENDACIÓN
	acuerdo con el plan y valida que la información de contacto sea correcta. Lo anterior, en aras de dar cumplimiento a las buenas prácticas para el desarrollo de simulacros del Plan de continuidad del Negocio descritos en la Norma ISO 22301 Sistemas de gestión de continuidad del negocio, además de MIPG V5 de 2023, Dimensiones 3 Gestión con Valores para Resultados y 5 Información y Comunicación, minimizando la materialización de riesgos asociados con R029 - Fallas en la Administración PCN y R102 - Fallas en Planes de Contingencia.
4	**Recomendación 4.** La OFCIN recomienda a OAGRI en coordinación con el proveedor de la herramienta VIGIA RERO, revisar y analizar la posibilidad de construir y unificar en el perfil de Auditor, la funcionalidad de consulta a todas las bondades de la aplicación como una opción de mejora a dicho software y de esta manera no limitar el desarrollo del ejercicio auditor. Igualmente, que se implemente el reporte automático de REROS que permita generación de éstos por periodos determinados, incluyendo datos de la especificación de los REROS y de las tareas llevadas a cabo para su resolución y demás trazabilidad. Lo anterior, con el objeto de permitir a la OFCIN la realización autónoma de las consultas, toma de evidencias y generación de reportes de información que considere pertinentes en la herramienta para el análisis de la información y documentación del informe de auditoría correspondiente.

Cordialmente

Fir
MA
2023/07/24 08:22:34

MARTHA CECILIA MORA CORREA
Jefe de la Oficina de Control Interno

Elaboró: Ing. Flor Alba Roncancio Gachancipá
Auditor Oficina de Control Interno.