INFORME AUDITORÍA No. 07 DE 2024
OAGRI - SEGURIDAD DE LA INFORMACIÓN CIBERSEGURIDAD (SARSICI), INCLUYE VALIDACIÓN ACCESIBILIDAD WEB NTC 5854:2011 – PERIODO AUDITADO DEL 01 DE MARZO DE 2023 AL 29 DE FEBRERO DE 2024

La OFCIN desarrolló el informe de Auditoría No.07 de 2024 OAGRI - Seguridad de la Información y Ciberseguridad (SARSICI), incluye validación accesibilidad WEB NTC 5854:2011, teniendo en cuenta los siguientes aspectos:

1. Introducción.

El propósito de este informe es entender como la Caja Promotora de Vivienda Militar y de Policía (CPVMP) administra el proceso motivo de la auditoría, considerando las iniciativas estratégicas a cargo, la estructura y la caracterización del proceso, integraciones con los sistemas de información y flujogramas que soportan la operativa, así como los riesgos y controles asociados.

La Seguridad de la Información y Ciberseguridad en Caja Honor, tiene como objetivo brindar las herramientas apropiadas para preservar la confidencialidad, integridad y disponibilidad de los sistemas de información, así como las políticas específicas para gestionar información en la Entidad.

2. Objetivo General.

La Oficina de Control Interno - OFCIN de Caja Honor en desarrollo de sus funciones constitucionales y legales, en cumplimiento del Programa de Auditoría para la vigencia 2024, adelantará auditoría al Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad - SARSICI, incluye validación NTC 5854:2011 en concordancia con la Circular Básica Jurídica 029 de 2014 – Parte I - Titulo IV, Capítulo 5 y la Circular Externa 007 de 2018 de la SFC y demás normatividad externa aplicable a la materia.

3. Alcance.

Verificar el cumplimiento de la Circular Básica Jurídica 029 de 2014 – Parte I - Titulo IV, Capítulo 5 y de la implementación de las 3 etapas requeridas por la Superintendencia Financiera de Colombia – SFC, en la Circular Externa 007 de 2018, para el periodo 01 de marzo de 2023 al 29 de febrero de 2024 y aspectos de la NTC 5854:2011, además de tener en cuenta en el desarrollo del ejercicio auditor las Normas Internacionales para el ejercicio profesional de Auditoría Interna NIA, controles en los procesos interrelacionados, guías, procedimientos, y demás documentación relacionada.

4. Marco Normativo.

4.1. Normativa Externa

- La Superintendencia Financiera de Colombia expidió, la regulación del SARO en el capítulo XXIII de la Circular Básica Contable y Financiera (Circular Externa 100 de 1995).

- Circular Externa 052 de 2007 de la Superintendencia Financiera de Colombia donde se establecen requerimientos mínimos de Seguridad y Calidad de la Información.

- Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia, Norma que regula las obligaciones mínimas que deben cumplir las Entidades destinatarias con el fin de promover mecanismos que protejan y aseguren las operaciones.

- Circular Externa Básica Jurídica 029 de 2014 – Parte I - Titulo IV, Capítulo 5 Requerimientos Mínimos para la Gestión de la Seguridad de la Información y la Ciberseguridad, de la SFC.

- Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia, establece las obligaciones que tiene las Entidades financieras de informar a los consumidores financieros sobre los incidentes de Ciberseguridad que se hayan presentado y en los cuales se viera afectada la confidencialidad y/o integridad de la información al igual que las medidas adoptadas para solucionar dicho incidente.

- Decreto 1078 de 2015 – Por el cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1008 de 2018 – Política de Gobierno Digital, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, "Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- Resolución 1519 de 2020 Ministerio de Tecnologías de la Información y las Comunicaciones, Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos

- Resolución 7870 del 2022 "Política General de Seguridad y Privacidad de la Información para el Sector Defensa" MDN.

- Norma ISO 31000:2009 Gestión del Riesgo, principios y directrices genéricas sobre la gestión del riesgo.

- Norma ISO 27032:2012 Gestión de la Ciberseguridad, Tecnologías de la Información - Técnicas de Seguridad - Directrices para la Ciberseguridad.

- Norma ISO 27001:2013 y Actualización 2022, Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

- NTC 5854:2011 Accesibilidad Web.

- Manual Operativo del MIPG, versión 4 de marzo de 2021.

- Manual Operativo del MIPG, versión 5 de marzo de 2023.

4.2. Normativa Interna

- GR-NA-MA-009 Manual Seguridad de la Información y Ciberseguridad, versión 3, aprobado el 25-06-2021.

- GR-NA-MA-003 Manual del Sistema de Administración de Riesgo Operacional - SARO, versión 17, aprobado el 02-02-2022, vigente hasta el 27-02-2024 puesto que se integró en el GR-NA-MA-010 Manual del Sistema Integral de Administración de Riesgos – SIAR V1 Aprobado el 27/Feb/2024, el cual entró en vigencia a partir del 27-02-2024.

- Procedimiento Gestión Administración de Usuarios de Red, Código IT-NA-PR-012, Versión 006 del 15/oct/2019.

- Procedimiento Gestión y Control de Licenciamiento, Código: IT-NA-PR-014, Versión: 006, del 9/dic/2020.

- Procedimiento gestionar acuerdos de niveles de servicio – ANS, Código: IT-NA-PR-003, Versión: 006 del 7/oct/2019.

- Procedimiento Detección y Análisis de Vulnerabilidades y Ethical Hacking, Código GR-NA-PR-028, Versión 4 del 22/oct./2018.

- Guía de Protocolo de Seguridad de la Información y Ciberseguridad para Home Office, Código GR-NA-GU-036, Versión 2 del 10/feb./2023.

- GR-NA-GU- 036 Guía de Protocolo de Seguridad de la Información y Ciberseguridad para Home Office, versión 3, aprobado el 06-07-2023.

- Guía Evaluación de Riesgos de Seguridad de la Información y Ciberseguridad, Código GR-NA-GU-018, versión 9 del 13/feb./2023.

- GR-NA-GU-018 Guía Evaluación de Riesgo de Seguridad de la Información y Ciberseguridad, versión 10, aprobado el 06-07-2023.

- IT-NA-GU-030 Guía de Gestión de Incidentes de Ciberseguridad, versión 4, aprobado el 28-06-2024.

- GR-NA-GU-023 Guía Gestión de Incidente de Seguridad de la Información, versión 9 aprobado el 06-07-2023.

- GR-NA-GU-017 Guía Borrado Seguro de la Información Código GR-NA-GU-017, Versión: 007 del 05/jul/2023.

- GR-NA-GU-015 Guía Gestión de Activos de Información, versión 7 aprobado el 06-07-2023.

- IT-NA-GU-025 Guía Portal Centro de Servicios, versión 8 de 28-jun-2023.

- GR-NA-GU-029 Guía Reporte General de Eventos de Riesgo, versión 6, aprobado el 06-jul-2023.

- Guía Gestión Seguridad en Redes, Código: IT-NA-GU-023, Versión 008 del 28/jun2023.

- Guía Aprobación de REROS en el sistema de información, Código GR-NA-GU-037, Versión 003 del 6/jul/2023.

- Guía de operación crear, modificar e inactivar usuarios y nombres de recursos de TI, Código: IT-NA-GU-009, versión: 016 del 28/jun/2023.

- Guía de operación generación de backups y proceso de restauración, Código IT-NA-GU-007, Versión: 017 del31/jul/2023.

- Guía Catálogo de servicios, Código: IT-NA-GU-021, Versión: 007 del 8/feb/2023.

- Guía Catálogo de servicios, Código: IT-NA-GU-021, Versión: 008 del 28/jun/2023.

- Formato Matriz de Riesgo SGSI, Código GR-NA-FM-029, Versión 009 del 6/jul/2023.

- GR-NA-FM-034 Formato Acuerdo de Confidencialidad y Política de Seguridad de la Información para la Relación Contractual, versión 7 aprobada el 06-Dic-2022.

- GR-NA-FM-034 Formato Acuerdo de Confidencialidad y Política de Seguridad de la Información para la Relación Contractual, versión 8 aprobada el 06-jul-2023.

- IT-NA-FM-004 Formato Adecuación y Destrucción de Información en Ambiente de pruebas, versión 15 aprobado el 06-12-2022.

- IT-NA-FM-004 Formato Adecuación y Destrucción de Información en Ambiente de pruebas, versión 16 aprobado el 28-jun-2023.

- Matriz Gestión Informática y Tecnológica, Código: IT-NA-MZ-001, Versión 015 del 28/jun/2023.

- Plan Estratégico de Tecnología de la Información (PETI), código IT-NA-PL-001, Versión 11 del 19/may/2020.

5. Resultado de la Evaluación.

5.1. Seguimiento a las recomendaciones y observaciones del anterior informe de Auditoría 07 de 2023 SARSICI.

Se revisa resultado de la última auditoría realizada a SARSICI - Informe de Auditoría No. 07 de 2023 - en el que se evidenciaron 3 oportunidades de mejora y se implementó el PMP correspondiente; el cual a la fecha de la presente auditoría se encuentran con un estado de avance del 80% de ejecución quedando pendiente la OMP3 la cual presenta fecha final Planificada para el 31/07/2024, tal como se muestra en la siguiente imagen:

Figura1 Estado PMP Auditoría SARSICI Informe 7 de 2023
Fuente: Suite Visión Empresarial (SVE), Consultado 15/04/2024

5.2. Respuestas recibidas de la solicitud de información.

Por parte de OAGRI

Teniendo en cuenta el requerimiento realizado el pasado 11 de marzo de 2024 a la Jefatura de OAGRI, con fecha 18-03-2024 se dispuso parte de la información requerida en el siguiente sitio compartido de SharePoint: DOCUMENTOS AUDITORIA SARSICI 2024, como se muestra en la siguiente imagen:

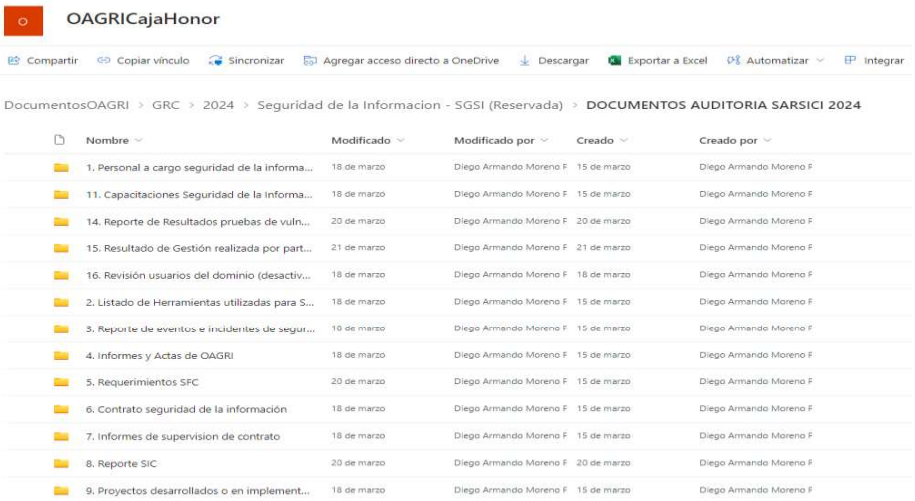


Figura 2 Archivos dispuesto por OAGRI en Repositorio Sharepoint
Fuente: Repositorio Documental Sharepoint *DOCUMENTOS AUDITORIA SARSICI 2024*

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

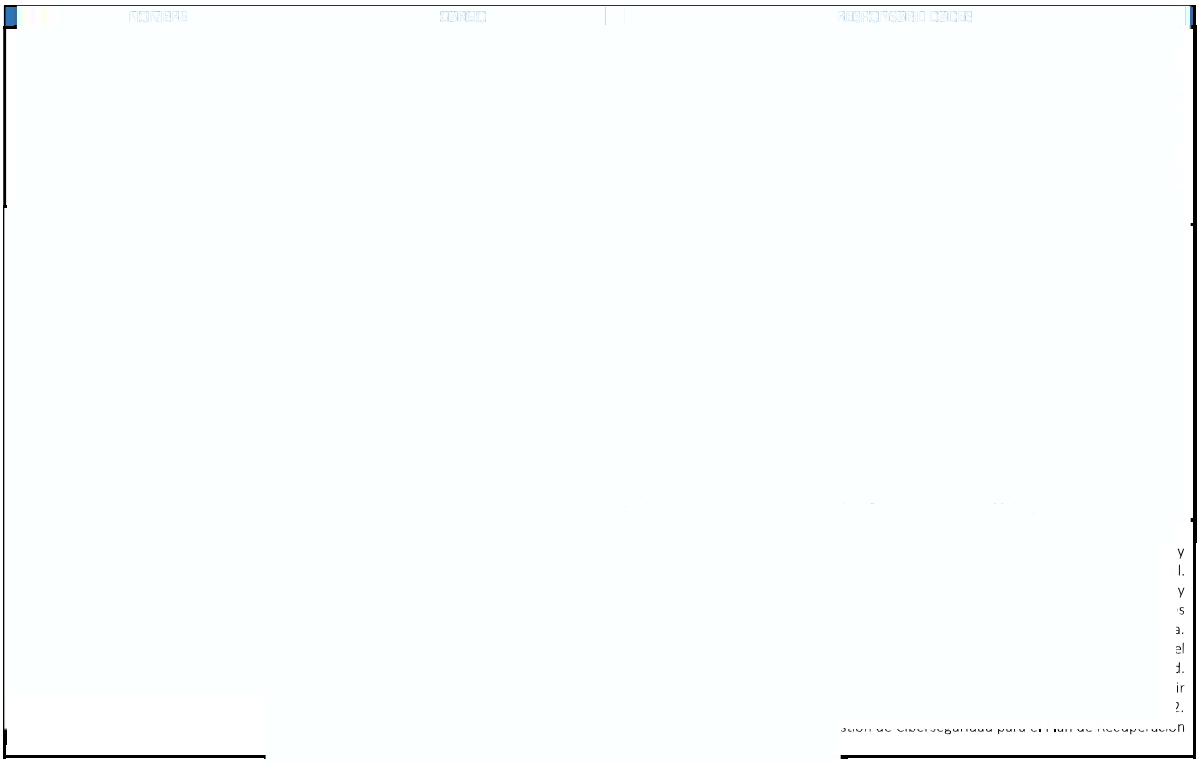
5.3.1. Personal a cargo de los procesos de Seguridad de la Información y Ciberseguridad

Información reportada por OAGRI

Figura3 OAGRI Relación de personal de Seguridad de la información y ciberseguridad
Fuente: Repositorio Documental Sharepoint *DOCUMENTOS AUDITORIA SARSICI 2024*

Información reportada por OAINF

Tabla 1 Relación de personal de ciberseguridad



Fuente: OAINF Email 18-04-2024

5.3.2. Herramientas tecnológicas utilizadas para seguridad de la información y Ciberseguridad

La MIDDLE OFFICE – OAGRI, cuenta con controles implementados para la mitigación de riesgos relacionados que en un momento dado pudiesen afectar la seguridad de la información en uno de sus principales pilares como lo es la confidencialidad, ya sea en reposo o en tránsito.

5.3.2.1. Herramientas de Monitoreo

En el proceso de revisión y entrevista con los colaboradores encargados de la Seguridad de la Información a nivel de OAGRI, se suministró información de las siguiente siguientes herramientas:

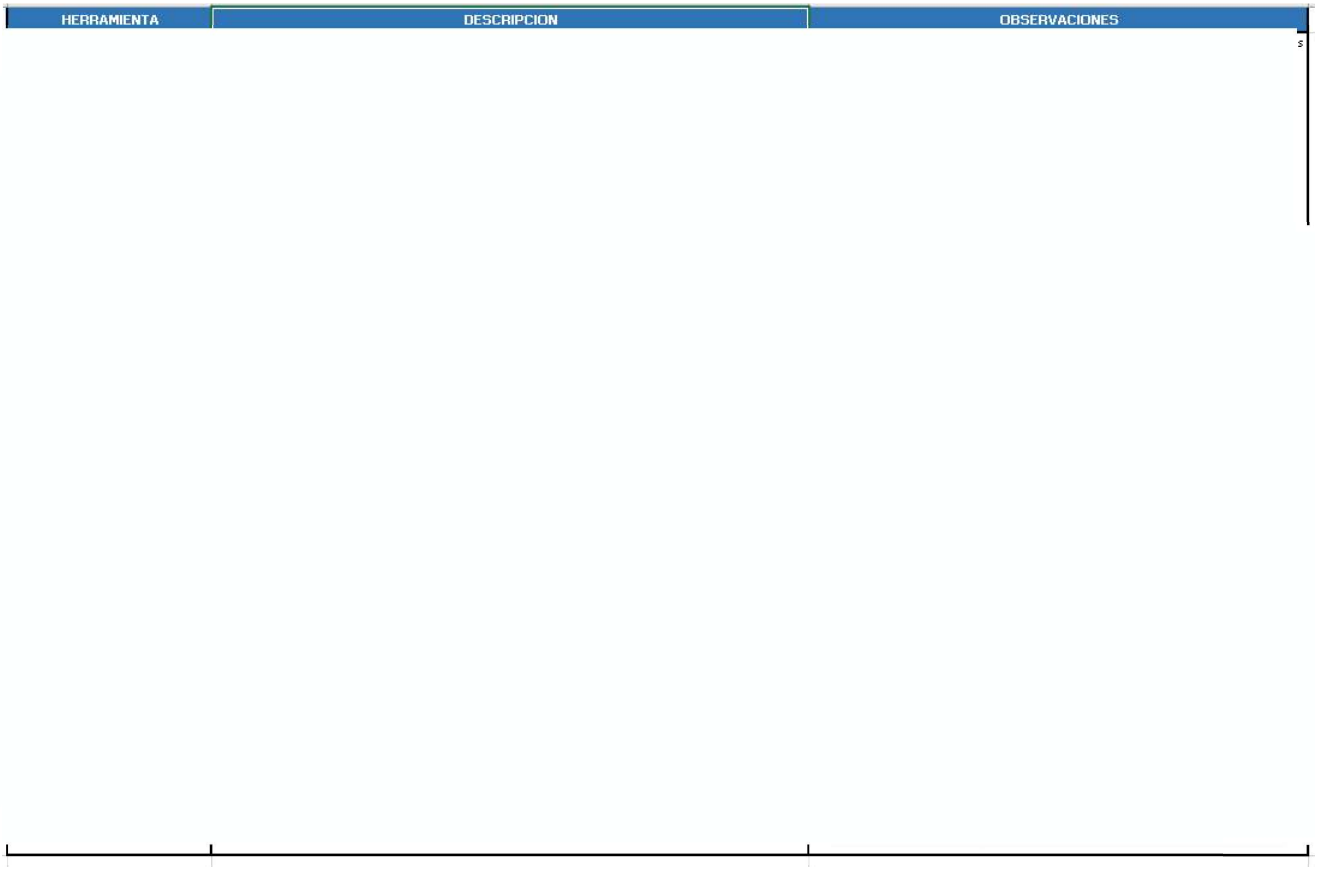


Figura 4 Lista Herramientas Tecnológicas para Seguridad de la información y Ciberseguridad
Fuente: Repositorio Documental Sharepoint *DOCUMENTOS AUDITORIA SARSICI 2024*

Desde la OAINF se suministró mediante email del 18-04-2024 la siguiente relación de herramientas tecnológicas utilizadas para desarrollar análisis de vulnerabilidades, tendientes a brindar seguridad fortaleciendo la infraestructura a nivel de redes y software:

Nombre	Funcionalidad	Licenciamiento	Observaciones
OSSIM	Diseñada para detección de intrusos y prevención y análisis de vulnerabilidades en la red	Licencia GLP	Se utiliza en la gestión de Seguridad de la Información
SonarQube	Inspección continua de la calidad del código a través de diferentes herramientas de análisis estático	Plataforma de Código abierto	

Nombre	Funcionalidad	Licenciamiento	Observaciones
OWAS ZAP	Utilizada como aplicación de seguridad y como herramienta profesional para pruebas de penetración	Plataforma de Código abierto	
Open Web Inspect de Fortify	Análisis Dinámico	Mediante adquisición del servicio de soporte y mantenimiento	Ciberseguridad
Estatic Code Analizar de Fortify	Análisis Estático		
System Security Center de Fortify	Analizador de Reglas y Funcionalidades		

Figura5 Herramientas de monitoreo suministradas por OAINF
Fuente Email 18-04-2024

5.3.3. Documentación controlada Seguridad de la Información y Ciberseguridad

Asimismo, se realizó consulta en la herramienta ISOLUCION de la documentación relacionada con los procedimientos de Seguridad de la Información y Ciberseguridad, evidenciando lo siguiente:

Ciberseguridad:

Figura6 Documentos asociados a Ciberseguridad
Fuente Isolución ® 5 Consultado 17-04-2024

Seguridad de la Información

Figura7 Documentos asociados a Seguridad de la Información
Fuente: Isolución ® 5 Consultado 17-04-2024

La OAGRI ha establecido e implementado cronograma de escaneo de vulnerabilidades tanto a los sistemas de información utilizados en Caja Honor para su Operación como a los portales Web, los cuales se presentan a continuación:

5.3.4. Cronograma Escaneos Vulnerabilidades

- **Cronograma de Escaneos Aplicativos Vigencia 2024**

Figura8 Cronograma Escaneo de Vulnerabilidades Aplicativos Caja Honor
Fuente: Repositorio Documental Sharepoint *DOCUMENTOS AUDITORIA SARSICI 2024*

En la Figura 8 se observa que durante el mes de enero de 2024 se realizaron escaneos de vulnerabilidades a las herramientas QUICKTURN VIRTUAL-CLIENT, GA2 y GA2+. Asimismo, en febrero de 2024 se realizó escaneo a la herramienta AFILIADO / FUNCIONAL KRITERION y en marzo de 2024 se aplicó escaneo de vulnerabilidades al aplicativo VISION y DODO-DOCS, en donde en el desarrollo del programa de auditorías 2024, la OFCIN requerirá para su análisis tales informes de resultados del proceso de escaneo de vulnerabilidades.

- **Cronogramas Escaneos Portales Web 2024**

En la figura 9 se observa que en los meses de enero y febrero se ha aplicado escaneos de vulnerabilidades a los sitios web que a continuación se mencionan: portal.cajahonor.gov.co, turnovirtual.cajahonor.gov.co, aplicacion.cajahonor.gov.co, www.cajahonor.gov.co y ex.cajahonor.gov.co, en donde la OAGRI suministró los correspondientes informes de resultados mediante los archivos citados a continuación:

- 2024-01-19-ZAP-Report-portal.cajahonor.gov.co.pdf: correspondiente al informe de resultados del escaneo al sitio: portal.cajahonor.gov.co, observando 4 alertas de nivel Medio y 3 de nivel Bajo, así:

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024

Así las cosas, la OFCIN procede a analizar las alertas de Nivel Medio:

Tabla 2 Report-portal.cajahonor.gov.co – Alertas Nivel Medio

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024

- ScanResult_20240119_SUFFIN

  Solo se identificaron alertas de nivel bajo e informativo.

- Cronograma Vulnerabilidades VLAN

  La OAGRI en coordinación con OAINF actualiza el cronograma de escaneos de la vigencia en donde el proveedor Wexler tiene como alcance los segmentos de red y sus nombres, a los cuales mediante técnica de caja gris (que son una combinación de pruebas de caja blanca y pruebas de caja negra, cuyo objetivo es buscar defectos debidos a una estructura incorrecta o al uso incorrecto de aplicaciones) realiza los escaneos respectivos generando los informes de resultados de vulnerabilidades, los cuales son remitidos por correo electrónico a la OAINF para el correspondiente análisis y aplicación de remediaciones. A continuación se presenta el cronograma planteado para la vigencia 2024, así:

Figura 10 Cronograma de Escaneo Vulnerabilidades VLANS
Fuente: Archivo Cronograma_VUL_&_EH_2024.xlsx - suministrado OAGRI Email 18-04-2024

Asimismo, con fecha 22-04-2024 la OAGRI dispuso en el repositorio SharePoint destinado para tal efecto, los archivos que a continuación se muestran, correspondientes a escaneos de vulnerabilidades aplicados en febrero de 2024 a las VLANS de la Entidad mediante la herramienta AlienVault: I.T Security Vulnerability Report, en ejecución del cronograma citado en la Figura 10, así:

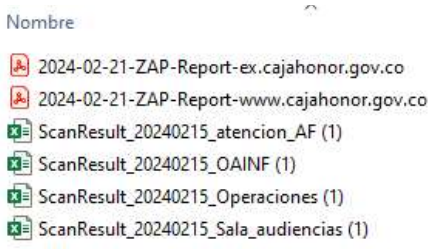


Figura 11 Reporte Escaneos de vulnerabilidades Feb-2024 a las VLANS Caja Honor
Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024

Así las cosas, la OFCIN toma un muestreo para análisis de la información, así:

- Archivo ScanResult_20240215_atencion_AF (1)

Contiene un total de 607 registros de IP escaneadas, en donde se observa la siguiente clasificación por nivel de riesgo:

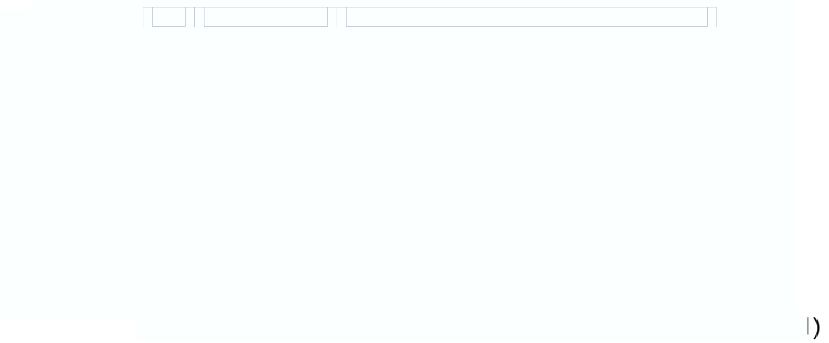
Tabla 5 Escaneo VLAN área Atención al Afiliado

Nivel de Riesgo	Cant.
Info	545
Low	50
Medium	12
Total general	**607**

Fuente: OAGRI Archivo ScanResult_20240215_atencion_AF (1)

Es de anotar que, las 12 alertas de Nivel Medio fueron halladas en las siguientes direcciones IP y corresponden a una misma alerta, como se muestra a continuación:

Tabla 6 Escaneo IP Atención al Afiliado - Alertas de Nivel Medio



)

Por lo anterior, la OFCIN recomienda aplicar las acciones de remediación pertinentes, las cuales para el caso analizado hacen referencia a deshabilitar los protocolos TLSv1.0 y/o TLSv1.1 obsoletos e instalar los protocolos TLSv1.2+ tendientes a reducir al máximo posible los efectos del riesgo o peligro en cuestión.

- **Archivo ScanResult_20240215_OAINF (1).xlsx**

Contiene un total de 764 registros de IP escaneadas, en el cual se observa la siguiente clasificación por nivel de riesgo, en donde la OFCIN entra a analizar las alertas de Nivel Alto y Medio:

Tabla 7 Escaneo VLAN Oficina Asesora de Informática

Nivel de Riesgo	Cant.
High	3
Info	678
Low	44
Medium	39
Total general	**764**

Fuente: OAGRI Archivo ScanResult_20240215_OAINF (1).xlsx

Las 3 alertas de Nivel Alto fueron halladas en las siguientes direcciones IP y corresponden a los siguientes aspectos, como se muestra a continuación:

Tabla 8 Escaneo IP Atención al OAINF - Alertas de Nivel Alto

Fuente: OAGRI – Archivo ScanResult_20240215_OAINF (1).xlsx

Como se observa en la tabla 8, en la Columba “Remedición” registra la posible solución recomendada tendiente a reducir al máximo posible los efectos del riesgo o peligro en cuestión para cada una de las alertas halladas en el elemento BOGOTAINF68.

Por su parte, de las 39 alertas de Nivel Medio, 32 de ellas corresponden a alertas relacionadas con Detección de protocolos TLSv1.0 y TLSv1.1 obsoletos en donde la recomendación dada para su remediación hace énfasis respecto a deshabilitar los protocolos TLSv1.0 y/o TLSv1.1 obsoletos y reemplazarlos por los protocolos TLSv1.2+, tema que igualmente se encuentra registrado en el campo Columna “Remedición”, así:

Tabla 9 Escaneo IP Atención al OAINF - Alertas de Nivel Medio

ítem	Nombre Host	Host IP	Nivel de Riesgo	Vulnerabilidad	Remediación

- **Archivo ScanResult_20240215_Operaciones (1).xlsx**

Contiene un total de 504 registros de IP escaneadas, en el cual se observa la siguiente clasificación por nivel de riesgo, en donde la OFCIN entra a analizar las alertas de Nivel Alto y Medio:

Tabla 10 Escaneo VLAN Área de Operaciones

Nivel de Riesgo	Cant.
Info	449
Low	44
Medium	11
Total general	**504**

Fuente: Archivo ScanResult_20240215_Operaciones (1).xlsx

Las 11 alertas de Nivel Medio fueron halladas en las siguientes direcciones IP y corresponden a los siguientes aspectos, como se muestra a continuación:

Tabla 11 Escaneo IP Área de Operaciones - Alertas de Nivel Medio

- **Archivo ScanResult_20240215_Sala_audiencias (1)**

Contiene un total de 26 registros en donde las IP escaneadas corresponden a 192.168.203.1, 192.168.203.11 y 192.168.203.12, hallando alerta de nivel informativo y bajo.

Reporte Análisis de vulnerabilidades suministrados por OAINF

Mediante email del 17-04-2024 emanado del líder de ciberseguridad a nivel de OAINF, se suministró la siguiente información en relación con análisis de vulnerabilidades aplicados a las herramientas tecnológicas utilizadas en la operación de Caja Honor, así:

Vigencia 2023:

Figura 12 Reportes de escaneos Aplicativos Caja Honor
Fuente: OAINF – Email 17-04-2024 Archivo Análisis de Vulnerabilidades.zip Carpeta 2023

Vigencia 2024:

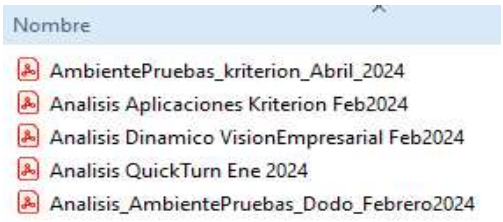


Figura 13 Reportes de escaneos Aplicativos Caja Honor
Fuente: OAINF – Email 17-04-2024 Archivo Análisis de Vulnerabilidades.zip Carpeta 2024

Así las cosas, la OFCIN procede a tomar un muestreo para análisis de la información, así:

- **Archivo AmbientePruebas_kriterion_Abril_2024.pdf**

En donde los profesionales de OAINF que realizaron el informe concluyen: “Se realizó el escaneo estático a la aplicación GA2, se visualiza que el código analizado compromete contraseñas y usuarios de las bases de datos, también llaves de acceso a Azure storage, esto puede llevar a accesos no autorizados, robo de información de las bases de datos, perdida de la disponibilidad de los servicios de GA2. Por parte de OAGRI se recomienda que se utilice algún método de cifrado para las contraseñas, usuarios y llaves de acceso para no comprometer la entidad; además no se puede identificar los hallazgos en falsos positivos porque no se puede comprobar que los métodos, campos que indica el proveedor que son privados son utilizados en la aplicación, en cuanto a las demás aplicaciones como GA2UEJ, se incrementó el número de hallazgos que estaban por subsanar a dos más, lo cual es de vital importancia su aminoramiento oportuno y la aplicación GA2APP, que no tenía hallazgos y se presentan dos hallazgos de contraseñas y de configuración por lo que es importante subsanar los hallazgos identificados como se explican en el presente informe.”

Recomendación 1.

Frente al informe reportado por OAINF mediante el archivo A**mbientePruebas_kriterion_Abril_2024.pdf**, es importante que dicho documento sea firmado tanto por los profesionales que lo elaboraron como por quien lo revisó; además de ser prioritario

que la OAINF en coordinación con OAGRI realicen el seguimiento al proveedor Kriterion y requerir evidencias de la aplicación de acciones tendientes a subsanar los hallazgos evidenciados.

- **Archivo Analisis_AmbientePruebas_Dodo_Febrero2024**

Fuente: Archivo Analisis_AmbientePruebas_Dodo_Febrero2024.pdf

En donde los profesionales de OAINF que realizaron el informe concluyen: “Se ejecutó el análisis a la aplicación Dodo en ambiente de pruebas donde se identificaron hallazgos de configuración para su pronto aminoramiento, se recomienda seguir las diferentes pautas indicadas en el presente informe siguiendo las recomendaciones y verificando el reporte adjunto de la aplicación de seguridad Web Inspec de Fortify, reporteAmbientePruebasDodo.pdf.”

Recomendación 2.

Frente al informe reportado por OAINF mediante el archivo Analisis_AmbientePruebas_Dodo_Febrero2024, es importante que dicho documento sea firmado

tanto por los profesionales que lo elaboraron como por quien lo revisó; además de ser prioritario que la OAINF en coordinación con OAGRI realicen el seguimiento respectivo y aplicación de acciones tendientes a subsanar los hallazgos evidenciados.

Respecto al tema de Escaneo de vulnerabilidades y una vez realizado el análisis de la información, la OFCIN realiza las siguientes precisiones:

Oportunidad de Mejora Correctiva 01.

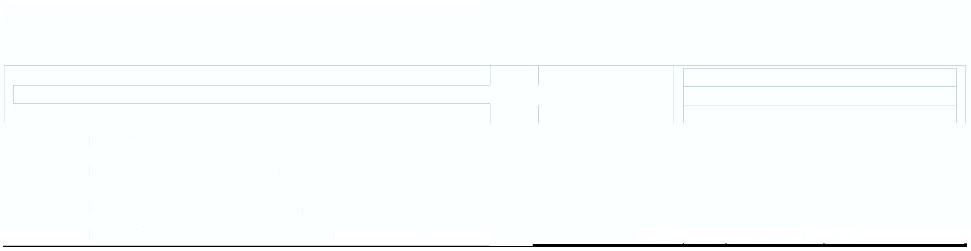
Se recomienda que: OAGRI en coordinación con OAINF y demás procesos interrelacionados gestionen los aspectos que a continuación se mencionan:

- Para no encontrar limitantes en el desarrollo del ejercicio auditor, suministrar oportunamente a la OFCIN tanto la información correspondiente a los Reportes de Escaneos de vulnerabilidades a los Aplicativos, Portales Web y VLANS como los Reportes de las Acciones aplicadas para su remediación.
- Los consultores de seguridad de la información del proveedor Wexler S.A. en sincronía con la OAINF deberán realizar los seguimientos respectivos al tema de subsanación de las vulnerabilidades (Cláusula 3 Obligación 5 Cto. 066 de 2022), toda vez que en la entrevista sostenida con el profesional de dicho contratista, se indicó que el proveedor Wexler realiza los escaneos y los entrega a la OAINF para la respectiva remediación, sin conocer y suministrar las evidencias de dichas subsanaciones. Para lo pertinente, debe presentarse el respectivo informe de remediaciones aplicadas.
- Asimismo es de vital importancia que la OAINF en coordinación con OAGRI realice el seguimiento respectivo al proveedor Kriterion solicitándole los soportes que den cuenta de la aplicación de acciones necesarias para la subsanación de las vulnerabilidades encontradas.
- La OAGRI en coordinación con OAINF deben asegurarse mediante la ejecución de un nuevo test, que se hayan subsanado todas las vulnerabilidades encontradas en los diferentes servicios, aplicativos, portales web, etc; con el objeto de determinar si aún persisten brechas de seguridad que puedan en un momento dado impactar de forma negativa a la Entidad, suministrando a la OFCIN el informe de resultados correspondiente.

Lo anterior, con el propósito de reducir al máximo posible los efectos del riesgo o peligro en cuestión para cada una de las vulnerabilidades halladas en los servicios o elementos escaneados en pro de preservar los criterios de seguridad de la información como son la Integridad, Confidencialidad y Disponibilidad de la misma garantizando a los afiliados de Caja Honor un adecuado uso y mantenimiento de sus datos en aras de dar cumplimiento a lo descrito en el Procedimiento Detección y Análisis de Vulnerabilidades y Ethical Hacking, código GR-NA-PR-028, V004 del 22-Oct-2018 el cual debe ser objeto de actualización no solo en su contenido sino en la normatividad vigente aplicable y responsables del mismo, Estándar ISO 27001:2013 y su actualización 2022, Resolución 7870 de 26-12-2022 “Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y continuidad de los servicios Tecnológicos” del MDN, entre otras NIA-N2120 Gestión de Riesgos, N-2130 Control y las buenas prácticas de Seguridad de la Información; minimizando la materialización de riesgos relacionados con R005 - Fallas en los Sistemas de Información, RSI008 - Error en el Uso, “R010 Incumplimiento de Obligaciones Legales y/o Normativas aplicables a la Entidad”, RSI030 - Información Errada, RSI031 - Pérdida de Información, Pérdida de Confidencialidad del Activo de Información, entre

otros, así como lo reglamentado en las Dimensiones de MIPG V5 de 2023, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.

Es de anotar que en entrevista con los colaboradores de la firma Wexler (consultor de seguridad de la información y analista de seguridad de la información) indican que a los portales web de la Entidad se les realiza monitoreo periódicamente generando un informe mensual, en donde las herramientas utilizadas para el análisis de vulnerabilidades son las citadas a continuación:



Fuente: OAGRI - Profesionales de Seguridad de la información firma Wexler – Entrevista 15-04-2024.

Por otra parte, se consultó en la herramienta ISOLUCION la documentación relacionada con la gestión y administración de portales institucionales controlados en Caja Honor, observando la siguiente documentación:

Figura14 Documentos asociados a servicios Portales Institucionales
Fuente: http://isolucion/IsolucionSig/Documentacion/frmListadoMaestroDocumentos.aspx, Consultado: Isolucion 18-04-2024.

Por otra parte, la OAINF mediante el correo electrónico del 19-04-2024 indica que desde la Oficina Asesora de Informática se utilizan para gestionar el tema de seguridad de la información y ciberseguridad, las siguientes herramientas:

Tabla 15 Herramientas Tecnológicas Seguridad de la información y Ciberseguridad - OAINF

Proceso	Herramienta	Funcionalidad	Licenciamiento

5.3.5. Contratos Seguridad de la Información y Ciberseguridad

La OAGRI suministró la siguiente relación de contratos de proveedores de servicios de seguridad de la información en Caja Honor:

Tabla 16 Relación de Contratos Proveedor Seguridad de la Información - OAGRI

ITEM	Vigencia	Numero	Vigencia	Objeto	Proveedor

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024

Respecto al ítem 1 (Otrosí No.1 Prorroga Cto. 066 de 2022), se observa que el mismo tuvo vigencia hasta el pasado 19 de abril de 2024; en donde para dar continuidad a la prestación del servicio se suscribió un nuevo contrato No. 031 de 2024 por un término de 12 meses.

Asimismo, la OAINF suministró la siguiente relación de contratos de proveedores de servicios de Seguridad de la Información y ciberseguridad, así:

Tabla 17 Relación de Contratos Proveedores Seguridad de la Información y Ciberseguridad - OAINF

ítem	Número de Contrato	Proveedor	Objeto del Contrato	Fecha finalización del contrato	Supervisor

5.3.6. Supervisión del Contrato

Una vez consultado en el gestor documental Dodo Docs el expediente contractual del proveedor Wexler S.A.S. se observa que los pagos correspondientes al periodo objeto de la presente auditoría corresponden del 11 al 23, como se muestra a continuación:

Figura 15 Proveedor Wexler SAS – Relación de pago marzo 2023 a marzo 2024
Fuente: Gestor Documental Dodo Docs – Consultado 25-04-2024

No obstante, no se evidencia informe como tal expedido por el supervisor del contrato al interior de Caja Honor para avalar los pagos, sino que en el expediente documental dentro del flujo 127-Expediente Contratos-Proveedores se encuentra asociado el flujo 179-Informes de Supervisión Contratos, el cual a su vez asocia el formulario 129-Proceso de pago a proveedores; el cual cuenta con un bloque correspondiente al registro del supervisor, así:

Es importante citar que respecto al contrato No. 066 de 2022 se encontraba desempeñando el rol de supervisor:

CLÁUSULA No.14 SUPERVISIÓN

La supervisión del presente contrato por parte de LA CAJA estará a cargo del Dr. Juan Manuel de Pio Doce Gómez Trujillo -Jefe Oficina Asesora de Gestión del Riesgo o quien hagas sus veces quien mediante el presente documento se le designa de tal función. En ausencia del supervisor, la supervisión la ejercerá el encargado o el superior inmediato.

Por su parte, para el contrato No. 031 de 2023 registra como supervisor el Jefe de la Oficina de Gestión de Riesgos entendiéndose que para la fecha se encuentra encargado de dicha área el Cr. Richard Oswaldo González Vera y a partir del 29-04-2024 ejercerá la supervisión de dicho contrato el Ing. Alejandro Perdomo Lozano.

Asimismo, tal como se describió en la tabla 17, desde la OAINF para los contratos relacionados con Seguridad de la Información y Ciberseguridad fueron designados para ejercer el rol de supervisor los ingenieros Profesional Especializado 4 y el Profesional Universitario 04.

Por otra parte, la OFCIN con fecha 07-05-2024 consultó el gestor documental Dodo Docs evidenciando la siguiente información de contratos de tecnología:

1. **Contrato 072 de 2022 ADVANTAGE MICROSYSTEMS COLOMBIA LTDA**

Figura 16 Contrato 072 de 2022 ADVANTAGE MICROSYSTEMS COLOMBIA LTDA
Fuente: Dodo Docs – Flujo 127-EXPEDIENTE CONTRATOS-PROVEEDORES - Consultado 07-05-2024

Figura 17 Otrosí Contrato 072 de 2022 ADVANTAGE MICROSYSTEMS COLOMBIA LTDA
Fuente: Dodo Docs – Flujo 127-EXPEDIENTE CONTRATOS-PROVEEDORES - Consultado 07-05-2024

No obstante, el tiempo transcurrido y las prórrogas dadas mediante los Otrosíes antes mencionados, la OFCIN no observa que el objeto contractual se encuentre en operación, es decir a la fecha el proveedor no ha hecho entrega del producto final que permita automatizar y optimizar la atención virtual de afiliados por parte de Caja Honor, tendiente a ofrecer un mejor servicio y respuesta inmediata a las consultas de los afiliados y que además permita analizar y comprender las preguntas y brindar respuestas precisas en cuestión de segundos; es decir, minimizando el tiempo que se tarda en resolver las inquietudes de nuestros afiliados. Lo anterior, redunda en el aumento de la productividad y ganancias para la Entidad puesto que reduce el margen de error e incrementa la calidad de los servicios.

2. **Contrato 121 de 2022 ADVANTAGE MICROSYSTEMS COLOMBIA LTDA**

Figura 18 Contrato 121 de 2022 Advantage Microsystems Colombia Ltda
Fuente: Dodo Docs – Flujo 127-Expediente Contratos-Proveedores - Consultado 07-05-2024

El Contrato 121 de 2022 presenta 3 modificaciones mediante los siguientes Otrosí:

Proveedor	No. Contrato	Objeto

Figura 19 Relación Otrosí Cto. 121 de 2022 Advantage Microsystems Colombia Ltda
Fuente: Dodo Docs – Flujo 127-Expediente Contratos-Proveedores - Consultado 07-05-2024

3. Contrato 045 de 2023 ADVANTAGE MICROSYSTEMS COLOMBIA LTDA

5. Contrato 220 de 2019 GRUPO KRITERION SAS

Una vez consultado el expediente contractual del presente contrato, se observa que el proveedor del software no ha dado cumplimiento al objeto contractual; es decir no ha incumplido los plazos

de los entregables del proyecto en los tiempos previamente establecidos y desde la vigencia 2020 a la fecha 07-05-2024 aún el contratista no ha hecho entrega del software o producto final. Es de anotar que en la ejecución del contrato No. 174-2020 se han suscrito 8 OTROSÍ, en donde se han modificado criterios relacionados con:

- El plazo de ejecución
- La cláusula número 3 – Obligaciones del Proveedor (relacionadas con contratación de personal especializado, tiempos de verificación de la información suministrada por Caja Honor, entre otros)

De igual manera, es de vital importancia la generación de informes de supervisión que den cuenta del seguimiento técnico, administrativo, financiero, contable y jurídico sobre el cumplimiento del objeto del contrato en la ejecución del mismo y suministro de entregables por parte del proveedor acorde a la planificación establecida para el desarrollo del proyecto, el cual sirve como insumo para la aprobación de pagos teniendo en cuenta lo establecido contractualmente. Es de anotar, que si bien es cierto, en el gestor documental Dodo Docs se ha implementado el Flujo 179-Informes de Supervisión de Contratos, en el mismo no se presenta un informe de supervisión propiamente dicho, en el cual se describan y anexen los soportes que den cuenta del cumplimiento por parte del contratista.

Asimismo, acorde a información suministrada por el Gerente del Proyecto desde la OAINF, se indica que el otrosí No. 8 se firmó el 30 de noviembre de 2023 y finaliza el 31 de mayo de 2024. De otra parte, teniendo en cuenta los seguimientos semanales que se están llevando a cabo al Proyecto Kriterion, el contratista presentó un diagrama en el que se cita la posible fecha en la que terminarían el proyecto, es así como se indica el 31 de agosto de 2024. No obstante, la OFCIN considera que el proyecto ha llevado demasiado tiempo y no se observa resultados positivos frente a la entrega de un software que cumpla las necesidades y expectativas de Caja Honor frente a la automatización de los procesos Core del negocio en aras de brindar beneficios a los afiliados y por tanto recomienda verificar desde la parte administrativa y evaluar el fundamento jurídico contractual, para hacer efectivas las pólizas por incumplimiento por parte del proveedor y/o demás instancias pertinentes referidas en el contrato.

Así las cosas, frente a los contratos de tecnología evaluados por la OFCIN, se tienen las siguientes precisiones:

Oportunidad de Mejora Correctiva 02.

La OFCIN recomienda a la OAGRI en coordinación con OAINF, ARCON, SUADM, proveedores de software y demás procesos interrelacionados, tomar las medidas a que haya lugar para dar celeridad al proceso de implementación y puesta en marcha de las herramientas Core del Negocio y Servicios para la Atención Virtual de afiliados, Sistema de Información Financiera ERP, que permita optimizar y mantener control en las operaciones de la Entidad garantizando contar en todo momento con información actualizada, verídica y con calidad tanto para los clientes internos y externos que la requieran; ofreciendo servicios de calidad a los afiliados a Caja Honor y a su vez atender requerimientos de Entes de Control como es el caso de la SFC relacionadas con "correcta aplicación de la jerarquía de pagos, los nuevos criterios definidos para el seguimiento de los inmuebles dados en leasing, la validación y/o ajuste al numeral 7.2.6.1.1. del Manual SARC y las decisiones y/o ajustes respecto a la aplicación de prepagos…". Asimismo, dar cumplimiento a lo descrito en el Estándar ISO 27001:2013 Gestión de Seguridad de la Información Anexo A numeral 12.A – Seguridad de las Operaciones y su actualización versión 2022, Circular Externa 052 de 2007 de la SFC donde se establecen requerimientos mínimos de Seguridad y Calidad de la Información, Circular Externa 042 de 2012 de la SFC, Norma que regula las obligaciones mínimas que deben cumplir las Entidades destinatarias con el fin de promover mecanismos que protejan y aseguren las operaciones, Circular Externa Básica Jurídica 029 de 2014 – Parte I - Titulo IV, Capítulo 5 Requerimientos Mínimos para la Gestión de la Seguridad de la Información y la Ciberseguridad, de la SFC, Circular 008 de 2023 SFC, Resolución 7870 del 2022 "Política General de Seguridad y Privacidad de la Información para el Sector Defensa" MDN, MIPG V5 de 2023, Dimensiones 3 Gestión con Valores para Resultados y 5 Información y Comunicación y demás normatividad aplicable en la materia; en aras de minimizar la materialización de riesgos asociados con RSI052 - No Disponibilidad de Herramientas de Consulta Para Gestionar Tramites por causas relacionadas con CSI010 - Inconsistencias del Software, RSI029 - Perdida de la Integridad del Activo de Información, RSI030 - información Errada, RSI031 - Perdida De información, RSI029 - Pérdida de la Integridad del Activo de información, RC02 - Alteración de información Reportada, CAC002 - Debilidades en el Seguimiento Periódico de las Actividades y Planes, RC19 - Manipulación del Contrato por parte del Supervisor del Mismo, CAC018 - Ejercer Presión sobre el Contratista con el fin de obtener un Beneficio Particular, RC26 - Fuga de Información, CAC025 - Fallas en la Clasificación de la Información y su Definición de Criticidad, entre otros.

5.3.7. Requerimientos recibidos por Entes de Control y su respectiva respuesta.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

La OAGRI con fecha 25-04-2024, dispuso en el Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 la carpeta 8.Reporte SIC/Seguimiento RNBD SIC 2023/BD SIC en la cual se evidencia informes de seguimiento de BD inscritas ente el SIC para los 4 trimestres de la vigencia 2023, dentro de dicho informe se observa la constancia de Bases de Datos finalizadas y pendientes por finalizar ante la SIC de trámite del reporte de incidentes que puedan poner en riesgo la información de los titulares de datos personales acorde a lo estipulado en la Ley 1581 de 2012; observándose en dicho documento vigencia 31 de marzo de 2024. Es de anotar que, el mismo documento constancia se encuentra

adjunto a cada periodo reportado. Así las cosas, la OFCIN indaga con el consultor de seguridad de la información de la OAGRI frente a la fecha de vigencia que presenta dicho documento, solicitando además se suministre soporte que evidencia el reporte de BD para cada uno de los periodos (Trimestres) suministrados como son mayo, septiembre y noviembre de 2023.

Figura 23 Constancia de reporte de BD ante la SIC VIGENCIA 2023.
Fuente: OAGRI- Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 la carpeta 8.Reporte SIC/Seguimiento RNBD SIC 2023/BD SIC

Por su parte, respecto a la vigencia 2024, la OAGRI dispuso la carpeta Seguimiento RNBD SIC 2024 en donde se observa el archivo Seguimiento BD inscritas en SIC (I trimestre 2024).docx correspondiente al informe de seguimiento del primer trimestre 2024, el cual contiene en su interior la siguiente constancia con fecha de vigencia a 31 de marzo de 2025, así:

Figura 24 Constancia de reporte de BD ante la SIC VIGENCIA 2024
OAGRI- Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 la carpeta 8.Reporte SIC/Seguimiento RNBD SIC 2024/BD SIC

No obstante, una vez observado el informe de seguimiento realizado por el proveedor Wexler, en entrevista con el consultor de seguridad de la información de dicha firma, se indica que no tiene conocimiento quien realiza al interior de Caja Honor el reporte de Bases de Datos ante la SIC, ni conoce las evidencias de cada periodo reportado puesto que en relación al tema, contractualmente solo se tiene la obligación de realizar el seguimiento, tarea que se evidencia mediante los informes que genera el consultor de manera trimestral. Entre tanto, la OFCIN manifiesta que si bien es cierto, contractualmente solo debe realizar seguimiento al tema, es importante que como buena práctica y comunicación efectiva, se mantenga sincronía con los colaboradores de Caja Honor encargados de realizar la actividad de reporte ante la SIC.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

- CIRCULAR EXTERNA 033 DE 2020 - REPORTE DE INFORMACIÓN PARA EL CÁLCULO DE MÉTRICAS E INDICADORES DE SI Y CS 4 TRIMESTRE 2022

La OAGRI, informa que acorde a los requerimientos de la SFC en la CE 033 de 2020, de forma trimestral (Finalizado el Trimestre Máximo a los 15 días siguientes) se debe radicar este requerimiento de información en la plataforma dispuesta por la SFC, para lo cual la OAGRI dispuso en el Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 Carpeta 5. Requerimientos SFC, la siguiente información que evidencia dicho trámite, correspondiente a la vigencia 2023:

Figura 25 Reporte Trimestral CE 033 de 2020 correspondiente a vigencia 2023

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta 5. Requerimientos SFC

Primer Trimestre 2023

Figura26 Reporte Primer Trimestre vigencia 2023 - CE 033 de 2020

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta_5. Requerimientos SFC

Evidencia de Envío

Figura 27 Evidencias Reporte Primer Trimestre vigencia 2023 - CE 033 de 2020

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta_5. Requerimientos SFC

Segundo Trimestre 2023

Figura 28 Reporte Segundo Trimestre vigencia 2023 - CE 033 de 2020
Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta 5. Requerimientos SFC

Evidencia de Envío

No se suministró evidencia del reporte a la SFC del segundo trimestre 2023

Tercer Trimestre 2023

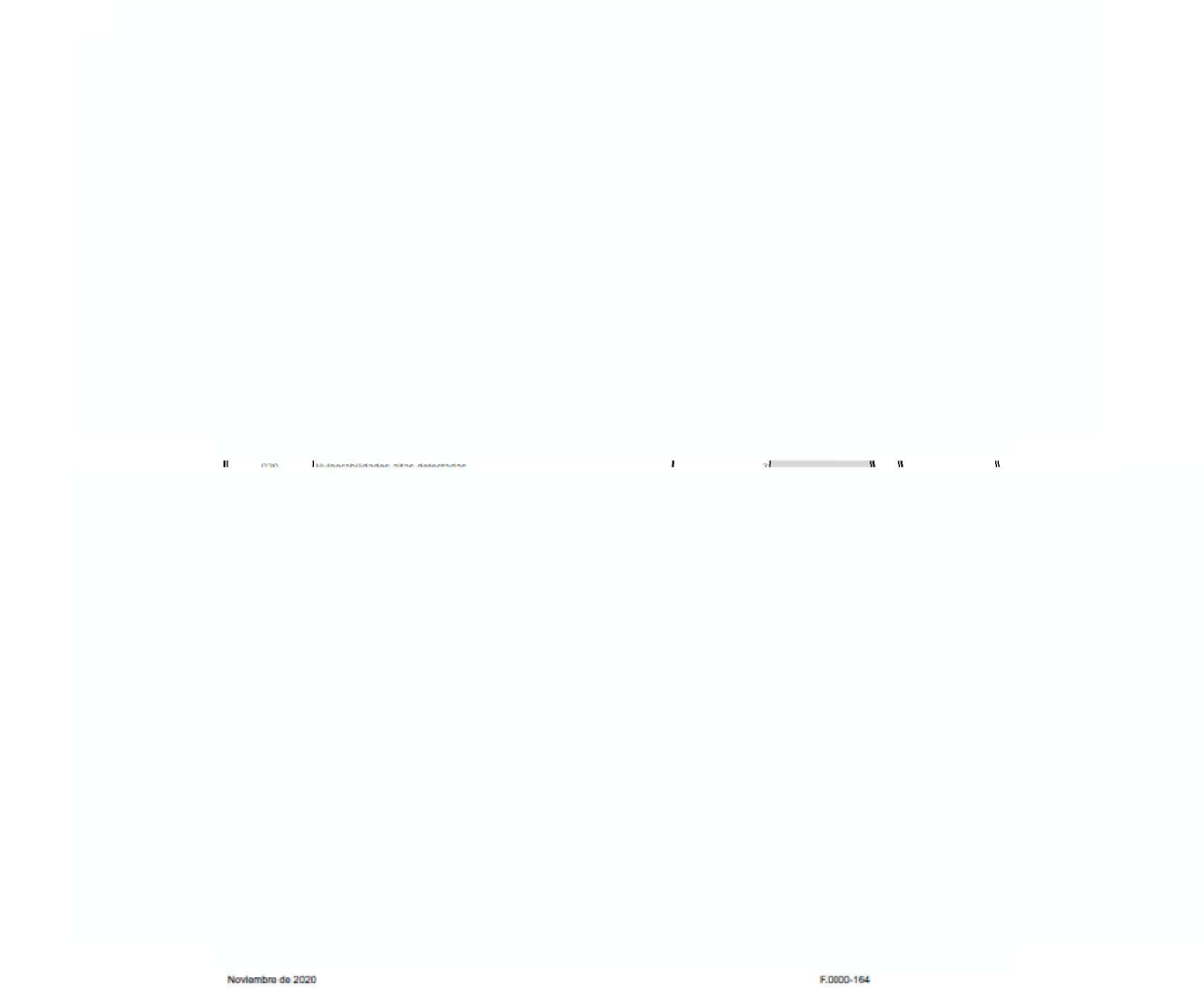


Figura 29 Reporte Segundo Trimestre vigencia 2023 - CE 033 de 2020

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta_5. Requerimientos SFC

Evidencia de Envío

Figura 30 Evidencia reporte Tercer Trimestre vigencia 2023 - CE 033 de 2020

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta_5. Requerimientos SFC

Cuarto Trimestre 2023

Figura31 Reporte Cuarto Trimestre vigencia 2023 - CE 033 de 2020
Fuente: : Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta 5. Requerimientos SFC

Evidencia de Envío

Figura 32 Evidencia Reporte Cuarto Trimestre vigencia 2023 - CE 033 de 2020
Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta 5. Requerimientos SFC

Acorde con la información antes presentada la OFCIN observó que la información correspondiente a los requerimientos realizados por la SFC mediante la CE 033 de 2020 fueron reportados de manera oportuna, excepto lo correspondiente al segundo trimestre 2023, en donde el proceso no suministro la evidencia respectiva.

Por su parte, la OFCIN ha indagado frente a otros requerimientos de la SFC como el caso que se presenta a continuación:

En donde el plazo improrrogable dado por la SFC frente al tema es el 30-Junio-2024, tal como se muestra en el siguiente oficio:

Con relación al presente requerimiento de la SFC, la OFCIN hace especial énfasis respecto a la celeridad en el proceso de implementación y puesta en producción del software Core del Negocio Kriterion, en donde con tiempo prudente se debe suministrar capacitación a la Oficina de Control Interno y conceder los accesos correspondientes para realizar las pruebas pertinentes al proceso de Aplicación de Pagos Extraordinarios (jerarquía de pagos en Leasing Habitacional, la aplicación

de prepagos y la información al deudor), asimismo, como lo menciona la SFC en el radicado 2022009160-072-000 del 03-May-2024, la validación y/o ajuste al numeral 7.2.6.1.1. del Manual SARC. Bajo las premisas citadas por la SFC, la OFCIN reitera la importancia que de manera prioritaria entre en producción la herramienta Core del Negocio que contenga todos los aspectos técnicos, de seguridad y funcionalidad, tecnología de punta que permita la automatización de los procesos manteniendo en todo momento información actualizada, precisa, confiable y oportuna en aras de ofrecer a los afiliados de Caja Honor, un servicio seguro, eficiente y de calidad que redunde en beneficios y facilidad en los trámites efectuados por el cliente, creando en él una experiencia favorable y de gran satisfacción. Asimismo, que de manera prioritaria y con antelación se suministre a la OFCIN la inducción correspondiente a la verificación funcional de los requerimientos antes citados emanados de la SFC.

5.3.8. Proyectos desarrollados y/o en implementación relacionados a Seguridad de la Información y Ciberseguridad

La OAGRI suministró información relacionada en los siguientes archivos:

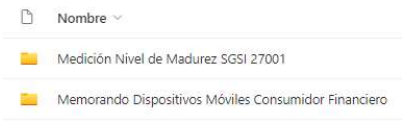


Figura 33 OAINF Proyectos Seguridad de la Información y Ciberseguridad

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 carpeta 9. Proyectos desarrollados o en implementación relacionado a Seguridad de la Información y Ciberseguridad

Carpeta Medición Nivel de Madurez SGSI 27001

Contiene el archivo Formato Análisis GAP ISO 27001 Recolección Evidencias_CAJAHONOR.xlsx correspondiente al diagrama de Gantt en el cual se presenta de manera gráfica los avances y porcentajes de cumplimiento de la estructura de alto nivel (93%) y Dominios del Anexo A (95%) en el proceso de implementación del Estándar ISO 27001:2013 en la Entidad, con corte a marzo de 2024.

Carpeta Memorando Dispositivos Móviles Consumidor Financiero

Contiene el archivo OAGRI-18-01-20231205002356 Política Uso Dispositivos Móviles - firmado.pdf emanado de la Gerencia General correspondiente a la Política uso dispositivos móviles para el consumidor financiero de Caja Honor.

5.3.9. Reporte de capacitaciones al personal

La OAGRI mediante el repositorio documental dispuso información concerniente a las capacitaciones, inducciones y actividades de ciberseguridad efectuadas en la vigencia 2023 y primer trimestre 2024, información suministrada en las siguientes carpetas:

Figura 34 Evidencia Capacitaciones Seguridad de la Información y Ciberseguridad
Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 Carpeta 11. Capacitaciones Seguridad de la Información y Ciberseguridad

A continuación se detallan las capacitaciones suministradas por la OAGRI a los colaboradores de la Entidad:

Tabla 18 Capacitaciones Seguridad de la Información y Ciberseguridad – Vigencia 2023

Ítem	Fecha	Proveedor	Objeto	Observaciones
1	ago-23	OAGRI - Wexler	Capacitación: Sensibilizar a funcionarios respecto a temas tales como: 1. La Seguridad de la Información tiene como objetivo principal proteger la: 2. La Ciberseguridad tiene como objetivo principal proteger la: 3. Son pilares de la Seguridad de la Información: 4. Cuál de las siguientes opciones no corresponde al cumplimiento de la política de escritorio limpio y pantalla limpia: 5. Consecuencias del incumplimiento de las políticas de Seguridad de la Información, entre otros.	Capacitacion Gestion de Vivienda
2	jun-23	OAGRI - Wexler	Capacitación: ¿QUE ES INFORMACION? Que busca preservar la seguridad de la información, Cual es la circular externa de la superintendencia financiera de Colombia la cual dicta como se debe clasificar la información a las entidades vigiladas como Caja Honor, Cuál es la clasificación de la información que determina la Superintendencia Financiera de Colombia, Cual es la ley que determina la clasificación de la información de Caja Honor, entre otros	Capacitación Virtual Seguridad de la Información OAGRI GAVIA
3	oct-23	OAGRI - Wexler	Capacitación: Temas: ¿QUE ES INGENIERIA SOCIAL?, ¿El phishing es una técnica de ingeniería social usada para obtener información persona o confidencial de forma fraudulenta?, ¿El vishing es una técnica de fraude o estafa, realizada a través de plataformas como Netflix o HBO?, ¿Los códigos QR son 100% seguros?, Si un mensaje de texto llega a mi celular, entre otros	Técnicas de Ingeniería Social
4	sep-23	OAGRI - Wexler	Capacitación	Seguridad de la Información preparación para la Auditoria ICONTEC
5	abr-23	OAGRI - Wexler	Capacitación	SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN-OAGRI
6	mar-23		Inducción: En materia de seguridad de la información, Ciberseguridad y PCN a funcionarios nuevos en la Entidad	En los meses de marzo, mayo, junio, julio, septiembre, octubre y diciembre se realizó Inducción: En materia de seguridad de la información, Ciberseguridad y PCN a funcionarios nuevos en la Entidad

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 Carpeta 11. Capacitaciones Seguridad de la Información y Ciberseguridad

Asimismo la OAGRI y el proveedor Wexler llevaron a cabo capacitaciones de Seguridad de la Información y Ciberseguridad durante el primer trimestre de 2024, tales como:

Tabla 19 Capacitaciones Seguridad de la Información y Ciberseguridad – Vigencia 2024

Ítem	Fecha	Proveedor	Objeto	Observaciones
1	ene-24	OAGRI - Wexler	Capacitación: REINDUCCIÓN POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	REINDUCCIÓN POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
2	ene-24	OAGRI - Wexler	Inducción 1. La Seguridad de la Información tiene como objetivo principal proteger la: 2. La Ciberseguridad tiene como objetivo principal proteger la: 3. Son pilares de la Seguridad de la Información: 4. Cuál de las siguientes opciones no corresponde al cumplimiento de la política de escritorio y pantalla limpios: 5. Consecuencias del incumplimiento de las políticas de Seguridad de la Información, entre otros.	Inducción a funcionarios nuevos de la Entidad
3	feb-24	OAGRI - Wexler	Capacitación: Sensibilizar a los funcionarios en temas de seguridad de la información y Ciberseguridad, aprender a identificar aquellos correos en donde el ciberdelincuente busca secuestrar la información	Capacitación SAC
4	feb-24	OAGRI - Wexler	Inducción 1. La Seguridad de la Información tiene como objetivo principal proteger la: 2. La Ciberseguridad tiene como objetivo principal proteger la: 3. Son pilares de la Seguridad de la Información: 4. Cuál de las siguientes opciones no corresponde al cumplimiento de la política de escritorio y pantalla limpios: 5. Consecuencias del incumplimiento de las políticas de Seguridad de la Información, entre otros.	Inducción a funcionarios nuevos de la Entidad
5	mar-24	OAGRI - Wexler	Capacitación: Seguridad de la Información e Ingeniería Social ARCOM	Seguridad de la Información e Ingeniería Social ARCOM

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 Carpeta 11. Capacitaciones Seguridad de la Información y Ciberseguridad

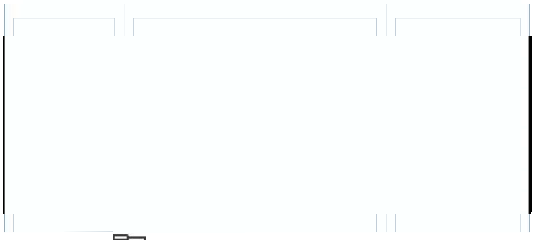
5.3.10. Reportes de eventos e incidente Seguridad de la Información, Ciberseguridad y Operacionales

Se informa por parte de OAGRI que en la vigencia 2023 los reportes de eventos / Incidentes se llevaba control manual en Excel, para lo cual dispuso en el repositorio compartido SharePoint la siguiente información:

Archivo Reporte de eventos e incidentes de seguridad de la información.xlsx.

La OAGRI suministró en el archivo antes citado la información correspondiente a un total de 146 registros de eventos e incidentes radicados en la herramienta Centro de Servicios durante la vigencia 2023, en donde a continuación se presenta la respectiva distribución por sede y Estado de los mismos, así:

Tabla 20 Reporte eventos e incidentes Seguridad de la Información y Ciberseguridad Vigencia 2023



Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 Carpeta 3. Reporte de eventos e incidentes de seguridad ciberseguridad y operaciones presentados

En prueba de recorrido con fecha 29-04-2024 con el consultor de seguridad de la información de OAGRI y el Técnico 04 de OAINF administrador de la herramienta Service Manager, la OFCIN observó que dicha herramienta aún no cuenta con un reporte automático que genere la relación de Eventos e Incidentes de un periodo dado, ni la identificación de si el registro corresponde a Evento o a Incidente, tema que, independientemente de si el usuario que registró el caso, lo colocó como Incidente o como Evento, es el consultor de seguridad de la información quien una vez analizado el caso, debe determinar en realidad a que corresponde. De igual forma, los comentarios tanto del seguimiento como del cierre son registrados en el campo "Nota". Así las

cosas, el Técnico 04 OAINF administrador del aplicativo Service Manager, genera una vista con campos específicos, organizando la información correspondiente al seguimiento, es decir separando la información registrada en el campo "Nota" en dos campos: "Comentario de Solución" y "Comentario de Cierre"; no obstante de los 146 registros citados en la Tabla 20 correspondientes a la vigencia 2023, se observó que un total de 66 registros, no presentan "Comentario de Cierre" y sin embargo su estado es "Cerrado".

Dados los anteriores comentarios, la OFCIN con el objeto de la mejora continua del proceso, hace especial énfasis respecto a:

Recomendación No. 3.

La OFCIN recomienda a la OAGRI en coordinación con la OAINF y demás procesos interrelacionados, verificar la posibilidad de implementar las funcionalidades antes citadas en la herramienta, puesto que este tema previamente había sido requerido por la OFCIN mediante la OMC1 registrada en el Informe Auditoría No. 07 de 2023, para lo cual el proceso suministró soportes de los avances al respecto y por tanto la OFCIN aprobó la tarea, sin embargo, en ejercicio de la presente auditoría se evidencia que las opciones implementadas (vista agregando los campos Texto1, Texto2 y Texto3) actualmente no son funcionales, puesto que no permiten la identificación precisa de la información).

5.3.11. Gestión de Usuarios (Definición de Accesos)

Con relación a la Gestión de Usuarios e identificación de accesos a las diferentes herramientas utilizadas en la Entidad para la ejecución de sus procesos, es importante que la Entidad cuente con una Matriz de Roles / Perfiles / Permisos que permita la parametrización de los accesos de usuarios alineados con la Matriz de Segregación de Funciones, es decir acorde a las actividades asignadas en el desempeño de sus funciones.

La OFCIN observa que respecto a proceso de levantamiento de información y documentación de matrices de Roles, Perfiles y Permisos de las diferentes herramientas tecnológicas utilizadas en la operación de la Entidad, en la vigencia 2022, la OFCIN registró el Plan de Mejoramiento por Proceso - SARSICI del 01-07-2021 al 31-10-2022, incluye NTC 5854:2011 producto de ejercicio auditor 12-2022, en donde se documentó la OMP1:

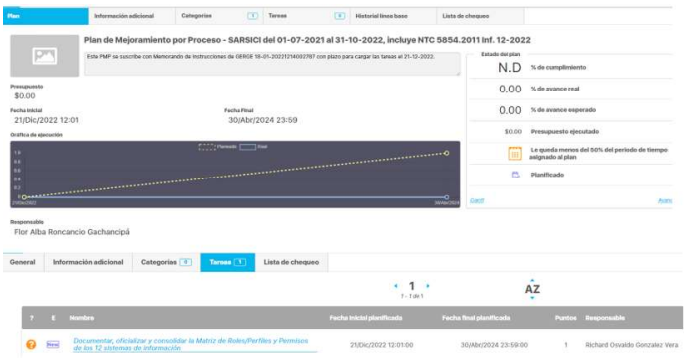


Figura 35 Oportunidad de Mejora OMP1 – OAGRI de 24-12-2022 – Consultado 30-04-2024
Fuente: Herramienta SVE – Plan de Mejoramiento por Proceso - https://vision/suiteve/base/client?soa=6&_sveVrs=965020221001&

Tendiente a dar cumplimiento a lo requerido por el Estándar ISO 27001:2013 en el Numeral 5.3. Roles, Responsabilidades y Autoridades en la Organización, su el Anexo A Numeral A.9. Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios y con las buenas prácticas de seguridad de la información. Es de anotar, que el plazo inicial se registró para el 30-Junio-2023 y mediante Email del 05-01-2024 la OAGRI solicitó un segundo plazo hasta el 30-Dic-2023 y posteriormente la OAGRI ha solicitado un tercer plazo para Documentar, oficializar y consolidar la Matriz de Roles/Perfiles y Permisos de los 12 sistemas de información hasta el próximo 30-Abril-2024.

Por su parte, respecto al mismo tema, se observa la existencia de la acción de mejora No. 408 aperturada el 24-06-2022 producto de la Auditoría Interna de Calidad de la Norma ISO 27001:2013 y con fecha de cierre proyectada al 22-12-2022, como se muestra a continuación:

Figura 36 Oportunidad de Mejora 408 – OAGRI de 24-06-2022 – Consultado 30-04-2024
Fuente: Herramienta Isolucion – Auditorías Internas SGI - ISO 27001:2013 link: *Isolución - Oportunidad de mejora No. 408*

Se observa que la Oportunidad de Mejora 408 – OAGRI de 24-06-2022 se encuentra cerrada con fecha 16-01-2023, no obstante, que a la fecha del presente informe aún no se encuentra documentada e implementada la Matriz de Roles, Perfiles y Permisos.

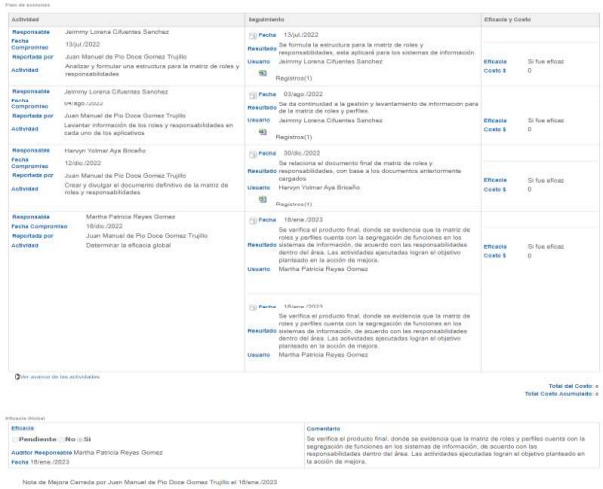


Figura 37 Plan de Acción - Oportunidad de Mejora 408 – OAGRI de 24-06-2022
Fuente: Isolucion – Consultado 30-04-2024 – link: *Isolución - Oportunidad de mejora No. 408*

Recomendación 4.

Teniendo en cuenta que la Oportunidad de Mejora 408 – OAGRI de 24-06-2022 se cerró sin tener documentada y socializada la completitud de la Matriz de Roles, Perfiles y Permisos de los aplicativos utilizados en la operación de la Entidad, en tanto que, únicamente se observa documento en Excel correspondiente a la Matriz de Roles para el Aplicativo GA2, la OFCIN recomienda revisar minuciosamente previo al cierre de las OM la subsanación de lo requerido en las Oportunidades de mejora atacando la causa raíz de su originación.

Por otra parte, es de anotar que, el proceso OAGRI mediante el email que a continuación se presenta, solicitó ampliación de fecha para la subsanación de OPM #1 PMP SARSICI Informe 12 de 2022 sobre roles y perfiles de todos los sistemas de información de la Entidad, plazo que finalizó el pasado 30 de abril de 2024, sin que a la fecha se hayan cargado en la SVE los soportes o evidencias respectivas:

Figura 38 Solicitud ampliación fecha para la subsanación de OPM #1 PMP SARSICI Informe 12 de 2022
Fuente: Correo electrónico emanado de OAINF – 05-01-2024

Por lo anteriormente expuesto, la OFCIN requirió mediante email del 03-05-2024 a la jefatura OAGRI el cargue en la SVE de los documentos oficiales de la citada matriz e igualmente se informe el estado de implementación y socialización de la misma en Caja Honor:

Figura 39 OFCIN- Solicitud cargue soportes OPM #1 PMP SARSICI Informe 12 de 2022
Fuente: Correo electrónico de 03-05-2024 enviado a OAGRI

Tema que será revisado de manera continua por la OFCIN para el cierre del PMP antes mencionado y en las próximas auditorías internas verificando la funcionalidad y operatividad de los perfiles y permisos implementados en las diferentes herramientas tecnológicas utilizadas para la operación de la Entidad.

5.3.12. Lista de usuarios registrados en el AD con fecha de corte al 28-02-2023.

El proceso no suministró información relacionada generando con ello una limitación frente al análisis de este ítem.

5.3.13. Documento Plan Estratégico de Tecnologías de la Información – PETI

Teniendo en cuenta que la OAINF no suministró información relacionada para el periodo auditado, la OFCIN procede a consultar en la herramienta Isolucion el documento Plan Estratégico de Tecnologías de la Información – PETI, Cod. IT-NA-PL-001, aprobado 19/may./2020:

Proceso	Codigo	Titulo Documento	Sucursal	Plantilla	Version	L M D_ Revisa	L M D_ Aprueba	Fecha Aprobacion
GESTIÓN INFORMÁTICA	IT-NA-PL-001	PLAN ESTRATÉGICO DE TECNOLOGÍA DE LA INFORMACIÓN (PETI)	Nivel Global	Plan	11	Ricardo Ignacio Becerra Borras,Jaime Sebastian Rodriguez Camargo	Lina María Rendón Lozano	19/may./2020

No obstante, no fue posible su lectura puesto que presenta el siguiente mensaje:

Dado lo anterior, se consultó con OAINF y OAPLA respecto al tema, quienes indican que el documento publicado en el repositorio de documentación controlada Isolucion corresponde al periodo 2019 – 2022, entre tanto el PETI para el cuatrienio comprendido entre las vigencias 2023-2026 se encuentra en formulación y actualización para ser presentado a la Junta Directiva para su aprobación; en tal sentido, la OAINF está llevando a cabo mesas de trabajo sobre el tema.

Así las cosas y teniendo en cuenta que el periodo de vigencia de dicho plan ya finalizó al cierre de la vigencia 2022, la OFCIN hace especial énfasis respecto a que se aplique celeridad a dicha gestión y se esté muy pendiente de los tiempos establecidos en la Directiva Permanente No. 030 del 31 de octubre de 2016 para la definición, documentación y oficialización de la estrategia de gobierno TIC que será el mapa de ruta para los próximos 4 años, comprendidos entre 2023 y 2026, articulado con el Plan Nacional de Desarrollo 2023 - 2026 y alineado con la Visón de Caja Honor, el cual recoja los nuevos proyectos e iniciativas a nivel de tecnología informática, se actualice la normatividad vigente como es la de la SFC CBJ Circular Externa 029 de 2019 en donde se imparten instrucciones tales como:

1. Modificar el subnumeral 3.5 del capítulo VI, título I, parte I "Reglas relativas al uso de servicios de computación en la nube" de la Circular Básica Jurídica, respecto del modelo de servicios SaaS.

2. Modificar el capítulo I del título II de la parte I de la Circular Básica Jurídica para incorporar instrucciones relativas a la implementación y uso de factores biométricos en la prestación de servicios financieros y adicionar instrucciones respecto de la seguridad y calidad para la realización de operaciones.

3. Adicionar el subnumeral 3.2.3.4 y modificar el subnumeral 3.2.4.6 del capítulo I del título III de la parte I de la Circular Básica Jurídica respecto de las condiciones para el intercambio de información y la generación de soportes al momento de realizar operaciones monetarias.

Circular Externa 033, del Noviembre 17 de 2020, la Superintendencia Financiera Imparte instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos – TUIC, el formato para el reporte de métricas de seguridad de la información y ciberseguridad y el protocolo de etiquetado para el intercambio de información Traffic Light Protocol, TLP.

Verificar la pertinencia de la Directiva Presidencial 04 de 2012, "Eficiencia administrativa y lineamientos de la política cero papel en la administración pública".

Decreto 444 del 29-03-2023 Racionalización de papel CONPES 3520 DE 2008

Y demás normatividad vigente en la materia que le aplique a la Entidad.

5.3.14. Bitácora de Backups / Restore

El proceso auditado no suministró información relacionada, lo que limita el análisis del tema en el desarrollo del ejercicio auditor.

5.3.15. Proceso de Ofuscamiento de Bases de Datos

Mediante Email del 11-03-2024 la OFCIN requirió al proceso auditado información relacionada con "Teniendo en cuenta que en Caja Honor existen diferentes proveedores de Servicios (software, Infraestructura, Comunicaciones, etc.) a quienes se les debe suministrar Bases de Datos para la ejecución del acuerdo contractual, es importante que las mismas se entreguen ofuscadas bajo la técnica de seguridad para enmascarar datos sensibles. Así las cosas, se solicita el suministro de tales evidencias correspondientes al periodo evaluado.

- Procedimiento, instructivo o guías implementados en Caja Honor para el ofuscamiento de datos", como se muestra a continuación:

No obstante, el proceso auditado no suministro información relacionada que de cuenta de la implementación de dicho proceso en la Entidad en aras de garantizar la protección de la

confidencialidad, integridad y disponibilidad de la información descrita en el Estándar ISO 27001:2013, Numeral A.10 Criptografía del Anexo A y Numeral 8.11 Enmascaramiento de Datos de su actualización 2022. Así las cosas, la OFCIN realiza la siguiente precisión:

Oportunidad de Mejora Preventiva 03.

La OFCIN recomienda a la OAGRI en coordinación con la OAINF y demás procesos interrelacionados documentar e implementar el procedimiento relacionado con la ofuscación de Bases de Datos, en tanto que es una práctica esencial para asegurar la privacidad y la protección de la información sensible, orientado a mitigar riesgos de seguridad, cumplir con normativas legales y proteger contra accesos no autorizados; especialmente para el suministro de las mismas a Terceros o contratistas e incluso usuarios internos, tendiente a la protección contra amenazas internas en donde empleados o contratistas con acceso legítimo a la Base de Datos podrían intentar utilizar los datos de manera indebida. Lo anterior, puesto que la ofuscación de datos ayuda entre otros aspectos a:

- Proteger la información sensible como datos personales, financieros o de salud asegurando que incluso si los datos son accesados por personas no autorizadas, éstos no puedan ser comprendidos ni utilizados de manera malintencionada.
- Cumplimiento Normativo y Regulaciones
- Mitigación de Riesgos de Seguridad: La ofuscación agrega una capa adicional de seguridad en caso de una brecha de seguridad, reduciendo el impacto al asegurarse de que los datos expuestos no sean directamente utilizados por los atacantes.
- Reducción de exposición en entornos compartidos: Por ejemplo en entornos en la nube, la ofuscación de datos asegura que en caso de fallos en la segregación de datos, la información sensible no sea fácilmente accesible.
- Minimización del impacto de errores humanos: En caso de que datos sensibles sean expuestos accidentalmente, por ejemplo enviando por correo un archivo incorrecto, la ofuscación garantiza que los datos no sean fácilmente comprensibles o explotables.

Dando cumplimiento a requerimientos de la SFC, Circular Externa 052 de 2007 donde se establecen requerimientos mínimos de Seguridad y Calidad de la Información, Circular Externa 042 de 2012 de la SFC, Norma que regula las obligaciones mínimas que deben cumplir las Entidades destinatarias con el fin de promover mecanismos que protejan y aseguren las operaciones, Circular Externa Básica Jurídica 029 de 2014 – Parte I - Titulo IV, Capítulo 5 Requerimientos Mínimos para la Gestión de la Seguridad de la Información y la Ciberseguridad, Estándar ISO 27001:2013, Numeral A.10 Criptografía del Anexo A y Numeral 8.11 Enmascaramiento de Datos de su actualización 2022, Resolución 7870 de 26-12-2022 “Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y continuidad de los servicios Tecnológicos” del MDN, y las buenas prácticas de Seguridad de la Información; minimizando la materialización de riesgos relacionados con “R010 Incumplimiento de Obligaciones Legales y/o Normativas aplicables a la Entidad”, RSI030 - Información Errada, RSI031 - Pérdida de Información, Pérdida de Confidencialidad del Activo de Información, entre otros, así como lo reglamentado en las Dimensiones de MIPG V5 de 2023, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.

5.3.16. Informes y Actas de OAGRI a GERGE, OAPLA, Comités, Juntas y Otros Entes relacionados a Seguridad de la Información y Ciberseguridad.

Al respecto la OAGRI suministró los siguientes archivos correspondientes a Informe SARSICI de los cuatro trimestres de la vigencia 2023 y Actas de Comité de Riesgos de abril, julio y octubre

de 2023 y enero de 2024, llevados a cabo en forma trimestral; que dan cuenta de las evidencias de la gestión realizada frente al cumplimiento en los controles de Seguridad de la Información y etapas de Ciberseguridad a fin de obtener un correcto funcionamiento del SGSI y mantenimiento del mismo en la Entidad; tendiente a la mitigación de posibles riesgos que se presenten hacia los activos de la Información en Caja Honor, logrando así la preservación y protección de la confidencialidad, integridad y disponibilidad de la información en los ámbitos tanto físicos como tecnológicos, así:

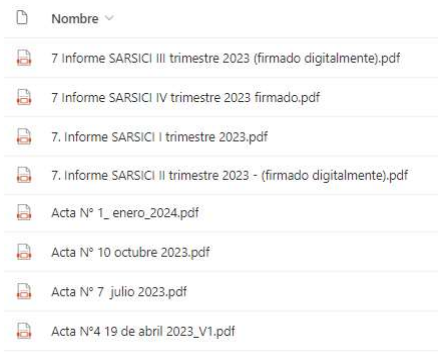


Figura 40 Informes y actas Gestión de Seguridad de la Información y Ciberseguridad

Fuente: Repositorio Documental Sharepoint DOCUMENTOS AUDITORIA SARSICI 2024 Carpeta 4. Informes y Actas de OAGRI

Es de anotar que en dichos informes trimestrales se plasma la gestión realizada por la OAGRI frente a aspectos tales como:

- Etapas de Gestión de Ciberseguridad.
- Prevención: controles creados y aplicados en el trimestre
- Protección, detección, comunicación, Recuperación y aprendizaje.
- Boletín informativo de Ciberseguridad.
- Reporte de ciberseguridad de los portales web de caja Honor:
  - Actividades de Protección contra Malware Avanzado
  - Seguimiento de indicadores del SGSI
  - Visita a proveedores críticos
  - Seguimiento roles y perfiles formularios y flujos Dodo Docs
  - Inducción Seguridad de la Información
  - Capacitación Seguridad de la Información

- Gestión de Seguridad Informática

  - Identificación de ciber amenazas

  a. Ethical Hacking y WPT

  b. Actividades de protección a la infraestructura tecnológica intrusión Prevention System

  - Actividades de protección de programa maligno por e-mail
  - Actividades de protección hacia los portales web de Caja Honor
  - Informe de eventos e incidentes de SGSI y Ciberseguridad

- Conclusiones y/o Recomendaciones

Asimismo, la Oficina Asesora de Gestión del Riesgo indica que continuará con el monitoreo, mejoras en los controles y actualización de anillos de seguridad de Caja Honor, en conjunto con el equipo de ciberseguridad de la OAINF, con el propósito de mantener toda la infraestructura tecnológica protegida, destacando las buenas prácticas de Ethical hacking realizadas. Se continua con la mejora continua en el SGSI a nivel normativo a fin de obtener el mejor desempeño y aplicación de la NTC 27001:2013 en la Entidad con el apoyo directo de las áreas tanto críticas como no críticas de Caja Honor para la prevención y protección de la Información.

5.3.17. Inventario de Hardware (Equipos de Cómputo)

No se suministró información relacionada por parte de la OAINF, lo que limita el análisis del tema en el desarrollo del ejercicio auditor.

No obstante, en aras de realizar el análisis de información respectivo, la OFCIN tomó la información de equipos de cómputo a corte febrero de 2024 suministrada por ALMAC mediante Email del 13-03-2024 en archivo denominado INFORME EQUIPOS DE COMPUTO FEBRERO 2024.xlsx, en donde se evidencia la siguiente información:

Tabla 21 Relación General de Equipos de Cómputo Caja Honor por dependencia corte Febrero de 2024

PROCESO / AREA	CANT.

PROCESO / AREA	CANT.

Fuente: ALMAC - Email del 13-03-2024 en archivo INFORME EQUIPOS DE COMPUTO FEBRERO 2024.xlsx

A continuación se presenta la distribución de equipos de cómputo por tipo de maquina (Portátil / Escritorio):

Tabla 22 Relación de Equipos de Cómputo Escritorio / Portátiles

Computador de Escritorio	
Descripción	Cant.
Total general	[illegible]

Computador Portátil	
Descripción	Cant.
Total general	[illegible]

Fuente: ALMAC - Email del 13-03-2024 en archivo INFORME EQUIPOS DE COMPUTO FEBRERO 2024.xlsx

6. ACCESIBILIDAD WEB

La OFCIN procedió a consultar la resolución 084 del 02-02-2022 en su **Artículo 17. Misión y Funciones del Área de Comunicaciones numeral 3.** Administrar y actualizar la página web, intranet, redes sociales y demás herramientas de comunicación, dando a conocer los modelos de solución de vivienda, productos, trámites y servicios de la Entidad, según la normativa vigente, se observa que ARCOM tiene asignado el Rol de Administrador Web.

Figura 41 Funciones Profesional Universitario 014 – ARCOM
Fuente: Herramienta Teams documento recibido 02-05-2024

Así las cosas, será el Profesional Universitario 01 de ARCOM quien se encargará de programar y mantener el sitio web para que funcione correctamente, aplicando actualizaciones de los requisitos normativos, etc., ofreciendo un sitio web fácil de usar y que brinde una experiencia segura y agradable a los usuarios.

Por su parte, teniendo en cuenta que el actual sitio web de la Entidad se encuentra implementado sobre la plataforma SharePoint versión 2013, la OFCIN nuevamente con fecha 06-05-2024 procede a consultar en internet en la página de Microsoft, el tema de soporte técnico de dicha versión, observando el siguiente mensaje "El soporte técnico para Office 2013 finalizó el 11 de abril de 2023 y no habrá ninguna extensión ni actualizaciones de seguridad extendidas", como se muestra a continuación:

Figura 42 Pantalla vigencia SharePoint 2013
Fuente: https://support.microsoft.com/es-es/office/fin-del-soporte-t%C3%A9cnico-para-office-2013-90e4b0d1-098f-4656-b6e7-8b13b67ed62f#:~:text=El%20soporte%20t%C3%A9cnico%20para%20Office,ni%20actualizaciones%20de%20seguridad%20extendidas.

En consecuencia, al no contar con la versión de SharePoint actualizada ni soporte por parte del proveedor Microsoft, no se garantiza el correcto funcionamiento del sitio Web ni se preservan los pilares fundamentales de Seguridad de la Información como son Confidencialidad, Integridad y Disponibilidad de la misma, estando expuesto a brechas de seguridad relacionadas con:

- Vulnerabilidades de seguridad no parcheadas, es decir mayor riesgo de compromiso de cuentas, filtración de datos u otras violaciones de seguridad.

- Falta de nuevas funcionalidades y mejoras en tanto que se pierden ventajas de funciones y mejoras más recientes que facilitan el desarrollo de SharePoint.

- Posible incompatibilidad con SharePoint más reciente, puesto que la versión obsoleta de SharePoint podría no ser totalmente compatible con las últimas versiones de SharePoint.

- Problemas de rendimiento y estabilidad dado que por lo general el software más antiguo suele ser más lento, propenso a fallos y tener un rendimiento inferior.

- Dificultad para obtener soporte del proveedor, dado que Microsoft sólo proporciona soporte oficial para las versiones más recientes y las versiones anteriores compatibles. El soporte de versiones obsoletas es limitado.

- Mayor probabilidad de problemas técnicos puesto que el software desactualizado suele tener más bugs, conflictos de versiones y otros inconvenientes que pueden causar serios problemas.

- Opciones limitadas para actualizar en tanto que la transición de la solución a una versión más nueva de la herramienta puede ser más difícil y requerir más esfuerzo.

- Riesgo de costos de oportunidad elevados, en un alto porcentaje, el tiempo y los esfuerzos invertidos en mantener la solución compatible con una versión obsoleta de la herramienta podrían dedicarse mejor a la adopción de funcionalidades más actualizadas.

Por lo que la OFCIN enfatiza en la importancia de que la OAGRI en coordinación con OAINF, ARCOM y demás procesos interrelacionados atiendan de manera prioritaria lo descrito en la OMP3 del informe de Auditoría 07 de 2023:

Figura 43 OMP3 – SARSICI – 2023
Fuente: SVE – PMP Informe de Auditoría 07 de 2023

El cual se encuentra en Desarrollo y con fecha final 31-Julio-2024, como se muestra a continuación:

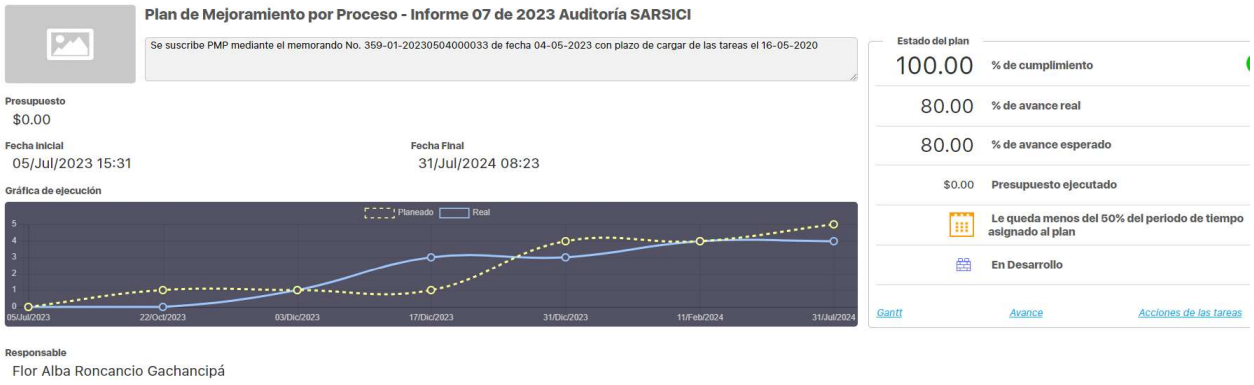


Figura 44 Plan de Mejoramiento por Proceso - Informe 07 de 2023 Auditoría SARSICI
Fuente: SVE – Consultado 06-05-2024

7. PUNTO ALTERNO DE CONTINUIDAD - PAC

Asimismo, mediante Email del 18-03-2024 la OFCIN requirió a la OAGRI y procesos interrelacionados información pertinente con el Punto Alterno de Continuidad- PAC, que asegure la recuperación de los procesos críticos que soportan la operación del negocio y su reanudación en el tiempo no mayor a los límites establecidos en la Guía de Análisis de Impacto del Negocio-BIA, en caso de presentarse alguna situación de desastre, de interrupción o contingencia que impida el acceso a las instalaciones de la Entidad y por ende el normal desarrollo de los procesos así:

Figura 45 Requerimiento de Información PAC
Fuente: OFCION Email 18-03-2024

Como respuesta al requerimiento de información citado en la Figura 3 la OAINF mediante email de 18-04-2024 suministro los siguientes archivos:

PERSONAL-PAC-PORTATIL-2024

Nombre

Es de anotar que, cada uno de los archivos corresponde al funcionario designado para el PAC y Formato Acuerdo de Confidencialidad para uso de dispositivos móviles y acceso remoto

Entre tanto, la OFCIN tomando la Base de Datos de personal de planta suministrada por ARTAH con corte al 31-12-2023, complementa el listado de personal asignado para el PAC, suministrado por OAINF, así:

Tabla 23 Personal asignado para Estrategia Trabajo Remoto - PAC

Por otra parte, la OFCIN mediante email del 16-04-2024 suministró el archivo Copia de PERSONAL-PAC-PORTATIL-2024.xlsx el cual contiene la siguiente información:

Tabla 24 Relación de personal designado para PAC - con Equipo Portátil en casa

Fuente: OAINF Email 16-04-2024 Archivo Copia de PERSONAL-PAC-PORTATIL-2024.xlsx

En la tabla 26 se puede observar que los únicos funcionarios que cuentan con equipo de cómputo en casa para Trabajo Remoto en caso de presentarse alguna situación de desastre, de interrupción o contingencia que impida el acceso a las instalaciones de la Entidad y por ende el normal desarrollo de los procesos son los que a continuación se mencionan:

En donde la OAINF indica mediante email del 16-04-2024 el "personal definido para PAC, y quienes ya tienen equipo asignado, los faltantes son los que están en proceso de compra y gestión con ARCON.

Asimismo, la OAINF suministró información requerida por la OFCIN con relación a la estrategia de trabajo remoto, así:

1. Medidas y controles de seguridad y ciberseguridad implementados en la operación de dichos equipos (conectividad, acceso a aplicativos, etc.) que garanticen la seguridad de la información procesada mediante la estrategia de trabajo remota.

   Respuesta OAINF:

   Mediante la estrategia de trabajo remoto, se tienen dispuestos una serie de controles como son los siguientes:

   a. Por defecto lo equipos tienen el Wi-Fi deshabilitado

b. Todo equipo antes de salir debe pasar por mesa de ayuda con el formato autorizado y firmado para que mesa de ayuda pueda: (Revisar que cumpla con los requisitos de Antimalware, Data Loss Prevention, Cifrado y finalmente le habilitan los servicios de WI-FI).
c. Seguido de esta actividad mesa de ayuda configura las tarjetas de red para que el equipo No navegue si no está conectada la VPN.
d. Una vez el equipo se encuentra conectado por trabajo remoto, toma todas las políticas tal cual las tiene asignadas en la oficina presencial.
e. Así mismo las actividades que intenten realizar fuera de los permisos asignados en cuanto al tema de fuga de información este opera en modo off line y on line, reportando las novedades en caso de presentarse a la OAGRI.

2. ¿Cuál es el procedimiento para el acceso remoto a servidores?

Respuesta OAINF:

El procedimiento que se realiza es:

a. Partiendo que los equipos que requiere acceder a un servidor (personal de T.I), debe estar en el entorno de la Red Lan, es decir bajos las políticas de la red de Caja Honor.
b. El primer paso es conectarse al PC que tiene asignado dentro de Caja Honor.
c. El segundo paso es una vez se encuentre bajo la Red Lan de Caja Honor es la única forma de conectarse a un servidor, previo que tenga el permiso requerido.
d. El tercer paso es que el servicio al cual requieran conectarse debe tener asignado el permiso del funcionario de T.I que se va a conectar.

Los usuarios finales no tienen acceso para realizar RDP (Protocolo de Escritorio Remo) a los servidores.

Por su parte, teniendo en cuenta lo anteriormente expuesto en el ítem 5.2.1. PUNTO ALTERNO DE CONTINUIDAD – PAC, la OFCIN realiza las siguientes precisiones:

Oportunidad de Mejora Preventiva 04.

La OFCIN recomienda a la OAGRI, en coordinación con OAINF y demás procesos interrelacionados documentar y actualizar la Guía del Usuario Punto Alterno de Continuidad (PAC), Cod. GR-NA-GU-005 / V 013 del 28-11-2023 y demás documentos que considere necesarios, en donde se incluya la propuesta para el manejo adecuado de las VPN, controles para el acceso remoto y demás aspectos concernientes con el tema PAC, además de ser importante hacer referencia a los anexos tales como:

1. Listado de personal designado para el PAC con datos mínimos como: Identificación, Nombres y Apellidos, Cargo en la Entidad, Proceso o Dependencia y Rol que ejerce en el PAC.

2. Listado actualizado de Equipos de Cómputo destinados para el PAC indicando Placa de Inventario, responsable y proceso asignado.

3. Copia Actualizada de los formatos de solicitud VPN debidamente diligenciados de cada uno de los colaboradores designados para el proceso PAC.

4. Medidas y controles de seguridad y ciberseguridad implementados en la operación de dichos equipos (conectividad, acceso a aplicativos, etc.) que garanticen la seguridad de la información procesada mediante la estrategia de trabajo remota.

5. Describir el procedimiento para el acceso remoto a servidores

- Siendo este tema de gran importancia, puesto que la documentación actualizada y a disposición de todos los usuarios que la requieran, brinda los procedimientos sustentables de operaciones mientras se lleva a cabo la recuperación del sistema de información luego de que este fue afectado por una amenaza; redundando en alcanzar la minimización del tiempo de inactividad y lograr mejoras sostenibles en la continuidad del negocio, la recuperación tras desastre de TI, las capacidades de gestión de crisis corporativas y la conformidad normativa. Asimismo, realizar las pruebas o simulacros periódicos del PAC para asegurar su funcionalidad. Lo anterior, dando cumplimiento a lo dispuesto por el Estándar 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 y su actualización versión 2022, 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, la Circular Externa 029 de 2014 de la SFC, 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, 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 008 de 2023 SFC, Resolución 7870 de 26-12-2022 “Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y continuidad de los servicios Tecnológicos” del MDN, GR-NA-MA-009 Manual Seguridad de la Información y Ciberseguridad, versión 3, aprobado el 25-06-2021, MIPG V5 de 2023, Dimensiones 3 Gestión con Valores para Resultados y 5 Información y Comunicación y demás normatividad aplicable en la materia; en aras de minimizar la materialización de riesgos asociados con R029 - Fallas en la Administración PCN, CA029 - Falta de Actualización y Capacitación de los Procedimientos Frente a la Normatividad; 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.

8. Conclusiones y/o Recomendaciones.

La OFCIN efectuó la evaluación al Sistema de Administración de Seguridad de la Información y Ciberseguridad, evidenciando el cumplimiento de lo establecido en la Circular Externa 007 de 2018 Parte I, Instrucciones generales aplicables a las Entidades vigiladas, Título IV Deberes y Responsabilidades, Capítulo V: Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, Circular Externa Básica Jurídica 029 de 2014 – Parte I - Titulo IV, Capítulo 5, emitidas por SFC, puesto que se evidencia continuo seguimiento tanto a la infraestructura tecnológica como a los canales de comunicación implementados, Circular Externa 052 de 2007 SFC, Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia, Norma que regula las obligaciones mínimas que deben cumplir las Entidades destinatarias con el fin de promover mecanismos que protejan y aseguren las operaciones, así como las normas complementarias que modifiquen, adicionen, reglamenten o sustituyan, Estándar ISO 27001:2013 y su actualization 2022, ISO 27032:2012 Gestión de la Ciberseguridad, Tecnologías de la Información - Técnicas de Seguridad - Directrices para la Ciberseguridad, con lo siguientes aspectos a destacar:

Conclusiones.

- ✓ La OFCIN recomienda mayor oportunidad y calidad en el suministro de la información por parte del proceso auditado, que le permita la verificación y análisis respectivo de información durante el ejercicio auditor, toda vez que se observaron diferentes limitaciones.

- ✓ La OFCIN observó que para la gestión concerniente con los procesos de Seguridad de la Información y Ciberseguridad de la plataforma tecnológica utilizada por Caja Honor para su operación, las dependencias responsables cuentan con el personal idóneo y las herramientas de monitoreo permanente 7x24 los 365 días del año, tendiente a la preservación de los pilares fundamentales de la seguridad de la información como son Integridad, Confidencialidad y Disponibilidad.

- ✓ Es de alta prioridad que la OAGRI en coordinación con OAINF y demás procesos interrelacionados atiendan y gestionen de manera oportuna y atacando la causa raíz que las origino, con el fin de que éstas no se vuelvan a presentar, para cada una de las Oportunidades de Mejora y Recomendaciones descritas en los planes de mejoramiento implementados como resultados de las auditorías internas realizadas.

- ✓ Se enfatiza la importancia de la entrada en producción de las herramientas Core del Negocio, Servicios de Atención Virtual y Sistema de Información Financiera ERP que cumplan con las necesidades de la Entidad y superen las expectativas de funcionalidad, modularidad, seguridad, actualización tecnológica, integraciones con otros sistemas de información, entre otros aspectos.

Como resultado del ejercicio auditor y en cumplimiento a las Directrices dadas por el DAFP relacionadas con MIPG, la OFCIN generó 4 Oportunidades de Mejora y 4 Recomendaciones tendientes a la mejora continua de los procesos.

#	OPORTUNIDADES DE MEJORA
1	**Oportunidad de Mejora Correctiva 01.** Se recomienda que: OAGRI en coordinación con OAINF y demás procesos interrelacionados gestionen los aspectos que a continuación se mencionan: - Para no encontrar limitantes en el desarrollo del ejercicio auditor, suministrar oportunamente a la OFCIN tanto la información correspondiente a los Reportes de Escaneos de vulnerabilidades a los Aplicativos, Portales Web y VLANS como los Reportes de las Acciones aplicadas para su remediación. - Los consultores de seguridad de la información del proveedor Wexler S.A. en sincronía con la OAINF deberán realizar los seguimientos respectivos al tema de subsanación de las vulnerabilidades (Cláusula 3 Obligación 5 Cto. 066 de 2022), toda vez que en la entrevista sostenida con el profesional de dicho contratista, se indicó que el proveedor Wexler realiza los escaneos y los entrega a la OAINF para la respectiva remediación, sin conocer y suministrar las evidencias de

	dichas subsanaciones. Para lo pertinente, debe presentarse el respectivo informe de remediaciones aplicadas. - Asimismo es de vital importancia que la OAINF en coordinación con OAGRI realice el seguimiento respectivo al proveedor Kriterion solicitándole los soportes que den cuenta de la aplicación de acciones necesarias para la subsanación de las vulnerabilidades encontradas. - La OAGRI en coordinación con OAINF deben asegurarse mediante la ejecución de un nuevo test, que se hayan subsanado todas las vulnerabilidades encontradas en los diferentes servicios, aplicativos, portales web, etc.; con el objeto de determinar si aún persisten brechas de seguridad que puedan en un momento dado impactar de forma negativa a la Entidad, suministrando a la OFCIN el informe de resultados correspondiente. Lo anterior, con el propósito de reducir al máximo posible los efectos del riesgo o peligro en cuestión para cada una de las vulnerabilidades halladas en los servicios o elementos escaneados en pro de preservar los criterios de seguridad de la información como son la Integridad, Confidencialidad y Disponibilidad de la misma garantizando a los afiliados de Caja Honor un adecuado uso y mantenimiento de sus datos en aras de dar cumplimiento a lo descrito en el Procedimiento Detección y Análisis de Vulnerabilidades y Ethical Hacking, código GR-NA-PR-028, V004 del 22-Oct-2018 el cual debe ser objeto de actualización no solo en su contenido sino en la normatividad vigente aplicable y responsables del mismo, Estándar ISO 27001:2013 y su actualización 2022, Resolución 7870 de 26-12-2022 “Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y continuidad de los servicios Tecnológicos” del MDN, entre otras NIA-N2120 Gestión de Riesgos, N-2130 Control y las buenas prácticas de Seguridad de la Información; minimizando la materialización de riesgos relacionados con R005 - Fallas en los Sistemas de Información, RSI008 - Error en el Uso, “R010 Incumplimiento de Obligaciones Legales y/o Normativas aplicables a la Entidad”, RSI030 - Información Errada, RSI031 - Pérdida de Información, Pérdida de Confidencialidad del Activo de Información, entre otros, así como lo reglamentado en las Dimensiones de MIPG V5 de 2023, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.
2	**Oportunidad de Mejora Correctiva 02**. La OFCIN recomienda a la OAGRI en coordinación con OAINF, ARCON, SUADM, proveedores de software y demás procesos interrelacionados, tomar las medidas a que haya lugar para dar celeridad al proceso de implementación y puesta en marcha de las herramientas Core del Negocio y Servicios para la Atención Virtual de afiliados, Sistema de Información Financiera ERP, que permita optimizar y mantener control en las operaciones de la Entidad garantizando contar en todo momento con información actualizada, verídica y con calidad tanto para los clientes internos y externos que la requieran; ofreciendo servicios de calidad a los afiliados a Caja Honor y a su vez atender requerimientos de Entes de Control como es el caso de la SFC relacionadas con “correcta aplicación

	de la jerarquía de pagos, los nuevos criterios definidos para el seguimiento de los inmuebles dados en leasing, la validación y/o ajuste al numeral 7.2.6.1.1. del Manual SARC y las decisiones y/o ajustes respecto a la aplicación de prepagos…". Asimismo, dar cumplimiento a lo descrito en el Estándar ISO 27001:2013 Gestión de Seguridad de la Información Anexo A numeral 12.A – Seguridad de las Operaciones y su actualización versión 2022, Circular Externa 052 de 2007 de la SFC donde se establecen requerimientos mínimos de Seguridad y Calidad de la Información, Circular Externa 042 de 2012 de la SFC, Norma que regula las obligaciones mínimas que deben cumplir las Entidades destinatarias con el fin de promover mecanismos que protejan y aseguren las operaciones, Circular Externa Básica Jurídica 029 de 2014 – Parte I - Titulo IV, Capítulo 5 Requerimientos Mínimos para la Gestión de la Seguridad de la Información y la Ciberseguridad, de la SFC, Circular 008 de 2023 SFC, Resolución 7870 del 2022 "Política General de Seguridad y Privacidad de la Información para el Sector Defensa" MDN, MIPG V5 de 2023, Dimensiones 3 Gestión con Valores para Resultados y 5 Información y Comunicación y demás normatividad aplicable en la materia; en aras de minimizar la materialización de riesgos asociados con RSI052 - No Disponibilidad de Herramientas de Consulta Para Gestionar Tramites por causas relacionadas con CSI010 - Inconsistencias del Software, RSI029 - Perdida de la Integridad del Activo de Información, RSI030 - información Errada, RSI031 - Perdida De información, RSI029 - Pérdida de la Integridad del Activo de información, RC02 - Alteración de información Reportada, CAC002 - Debilidades en el Seguimiento Periódico de las Actividades y Planes, RC19 - Manipulación del Contrato por parte del Supervisor del Mismo, CAC018 - Ejercer Presión sobre el Contratista con el fin de obtener un Beneficio Particular, RC26 - Fuga de Información, CAC025 - Fallas en la Clasificación de la Información y su Definición de Criticidad, entre otros.
3	**Oportunidad de Mejora Preventiva 03**. La OFCIN recomienda a la OAGRI en coordinación con la OAINF y demás procesos interrelacionados documentar e implementar el procedimiento relacionado con la ofuscación de Bases de Datos, en tanto que es una práctica esencial para asegurar la privacidad y la protección de la información sensible, orientado a mitigar riesgos de seguridad, cumplir con normativas legales y proteger contra accesos no autorizados; especialmente para el suministro de las mismas a Terceros o contratistas e incluso usuarios internos, tendiente a la protección contra amenazas internas en donde empleados o contratistas con acceso legítimo a la Base de Datos podrían intentar utilizar los datos de manera indebida. Lo anterior, puesto que la ofuscación de datos ayuda entre otros aspectos a: - Proteger la información sensible como datos personales, financieros o de salud asegurando que incluso si los datos son accesados por personas no autorizadas, éstos no puedan ser comprendidos ni utilizados de manera malintencionada. - Cumplimiento Normativo y Regulaciones

	- Mitigación de Riesgos de Seguridad: La ofuscación agrega una capa adicional de seguridad en caso de una brecha de seguridad, reduciendo el impacto al asegurarse de que los datos expuestos no sean directamente utilizados por los atacantes. - Reducción de exposición en entornos compartidos: Por ejemplo en entornos en la nube, la ofuscación de datos asegura que en caso de fallos en la segregación de datos, la información sensible no sea fácilmente accesible. - Minimización del impacto de errores humanos: En caso de que datos sensibles sean expuestos accidentalmente, por ejemplo enviando por correo un archivo incorrecto, la ofuscación garantiza que los datos no sean fácilmente comprensibles o explotables. Dando cumplimiento a requerimientos de la SFC, Circular Externa 052 de 2007 donde se establecen requerimientos mínimos de Seguridad y Calidad de la Información, Circular Externa 042 de 2012 de la SFC, Norma que regula las obligaciones mínimas que deben cumplir las Entidades destinatarias con el fin de promover mecanismos que protejan y aseguren las operaciones, Circular Externa Básica Jurídica 029 de 2014 – Parte I - Titulo IV, Capítulo 5 Requerimientos Mínimos para la Gestión de la Seguridad de la Información y la Ciberseguridad, Estándar ISO 27001:2013, Numeral A.10 Criptografía del Anexo A y Numeral 8.11 Enmascaramiento de Datos de su actualización 2022, Resolución 7870 de 26-12-2022 “Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y continuidad de los servicios Tecnológicos” del MDN, y las buenas prácticas de Seguridad de la Información; minimizando la materialización de riesgos relacionados con “R010 Incumplimiento de Obligaciones Legales y/o Normativas aplicables a la Entidad”, RSI030 - Información Errada, RSI031 - Pérdida de Información, Pérdida de Confidencialidad del Activo de Información, entre otros, así como lo reglamentado en las Dimensiones de MIPG V5 de 2023, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.
4	**Oportunidad de Mejora Preventiva 04.** La OFCIN recomienda a la OAGRI, en coordinación con OAINF y demás procesos interrelacionados documentar y actualizar la Guía del Usuario Punto Alterno de Continuidad (PAC), Cod. GR-NA-GU-005 / V 013 del 28-11-2023 y demás documentos que considere necesarios, en donde se incluya la propuesta para el manejo adecuado de las VPN, controles para el acceso remoto y demás aspectos concernientes con el tema PAC, además de ser importante hacer referencia a los anexos tales como: 1. Listado de personal designado para el PAC con datos mínimos como: Identificación, Nombres y Apellidos, Cargo en la Entidad, Proceso o Dependencia y Rol que ejerce en el PAC. 2. Listado actualizado de Equipos de Cómputo destinados para el PAC indicando Placa de Inventario, responsable y proceso asignado.

3. Copia Actualizada de los formatos de solicitud VPN debidamente diligenciados de cada uno de los colaboradores designados para el proceso PAC.

4. Medidas y controles de seguridad y ciberseguridad implementados en la operación de dichos equipos (conectividad, acceso a aplicativos, etc.) que garanticen la seguridad de la información procesada mediante la estrategia de trabajo remota.

5. Describir el procedimiento para el acceso remoto a servidores

- Siendo este tema de gran importancia, puesto que la documentación actualizada y a disposición de todos los usuarios que la requieran, brinda los procedimientos sustentables de operaciones mientras se lleva a cabo la recuperación del sistema de información luego de que este fue afectado por una amenaza; redundando en alcanzar la minimización del tiempo de inactividad y lograr mejoras sostenibles en la continuidad del negocio, la recuperación tras desastre de TI, las capacidades de gestión de crisis corporativas y la conformidad normativa. Asimismo, realizar las pruebas o simulacros periódicos del PAC para asegurar su funcionalidad. Lo anterior, dando cumplimiento a lo dispuesto por el Estándar 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 y su actualización versión 2022, 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, la Circular Externa 029 de 2014 de la SFC, 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, 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 008 de 2023 SFC, Resolución 7870 de 26-12-2022 “Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y continuidad de los servicios Tecnológicos” del MDN, GR-NA-MA-009 Manual Seguridad de la Información y Ciberseguridad, versión 3, aprobado el 25-06-2021, MIPG V5 de 2023, Dimensiones 3 Gestión con Valores para Resultados y 5 Información y Comunicación y demás normatividad aplicable en la materia; en aras de minimizar la materialización de riesgos asociados con R029 - Fallas en la Administración PCN, CA029 - Falta de Actualización y Capacitación de los Procedimientos Frente a la Normatividad; 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.

Fuente: Elaboración propia OFCIN, mayo de 2024.

#	RECOMENDACIONES
1	**Recomendación 1.** Frente al informe reportado por OAINF mediante el archivo ambientepruebas_kriterion_abril_2024.pdf, es importante que dicho documento sea firmado tanto por los profesionales que lo elaboraron como por quien lo revisó; además de ser prioritario que la OAINF en coordinación con OAGRI realicen el seguimiento al proveedor Kriterion y requerir evidencias de la aplicación de acciones tendientes a subsanar los hallazgos evidenciados.
2	**Recomendación 2.** Frente al informe reportado por OAINF mediante el archivo Analisis_AmbientePruebas_Dodo_Febrero2024, es importante que dicho documento sea firmado tanto por los profesionales que lo elaboraron como por quien lo revisó; además de ser prioritario que la OAINF en coordinación con OAGRI realicen el seguimiento respectivo y aplicación de acciones tendientes a subsanar los hallazgos evidenciados.
3	Teniendo en cuenta la prueba de recorrido con fecha 29-04-2024 con el consultor de seguridad de la información de OAGRI y el Técnico 04 de OAINF administrador de la herramienta Service Manager, la OFCIN observó que dicha herramienta aún no cuenta con un reporte automático que genere la relación de Eventos e Incidentes de un periodo dado, ni la identificación de si el registro corresponde a Evento o a Incidente, tema que, independientemente de si el usuario que registró el caso, lo colocó como Incidente o como Evento, es el consultor de seguridad de la información quien una vez analizado el caso, debe determinar en realidad a que corresponde. De igual forma, los comentarios tanto del seguimiento como del cierre son registrados en el campo "Nota". Así las cosas, el Técnico 04 OAINF administrador del aplicativo Service Manager, genera una vista con campos específicos, organizando la información correspondiente al seguimiento, es decir separando la información registrada en el campo "Nota" en dos campos: "Comentario de Solución" y "Comentario de Cierre"; no obstante de los 146 registros citados en la Tabla 18 correspondientes a la vigencia 2023, se observó que un total de 66 registros, no presentan "Comentario de Cierre" y sin embargo su estado es "Cerrado". Dados los anteriores comentarios, la OFCIN con el objeto de la mejora continua del proceso, hace especial énfasis respecto a: **Recomendación No. 3.** La OFCIN recomienda a la OAGRI en coordinación con la OAINF y demás procesos interrelacionados, verificar la posibilidad de implementar las funcionalidades antes citadas en la herramienta, puesto que este tema previamente había sido requerido por la OFCIN mediante la OMC1 registrada en el Informe Auditoría No. 07 de 2023, para lo cual el proceso suministró soportes de los avances al respecto y por tanto la OFCIN aprobó la tarea, sin embargo, en ejercicio de la presente auditoría se evidencia que las opciones implementadas (vista agregando los campos Texto1, Texto2 y Texto3) actualmente no son funcionales, puesto que no permiten la identificación precisa de la información).

4	**Recomendación 4.** Teniendo en cuenta que la Oportunidad de Mejora 408 – OAGRI de 24-06-2022 se cerró sin tener documentada y socializada la completitud de la Matriz de Roles, Perfiles y Permisos de los aplicativos utilizados en la operación de la Entidad, en tanto que, únicamente se observa documento en Excel correspondiente a la Matriz de Roles para el Aplicativo GA2, la OFCIN recomienda revisar minuciosamente previo al cierre de las OM la subsanación de lo requerido en las Oportunidades de mejora atacando la causa raíz de su originación.

Fuente: Elaboración propia OFCIN, mayo de 2024

En los anteriores términos la Oficina de Control Interno, da cumplimientos a lo establecido en el cronograma de auditoría 2024, encaminada a la mejora continua de los procesos.

Cordialmente.

Firmado por:
MARTHA CECILIA MORA CORREA
2024/05/27 09:37:01
CC
55165780

MARTHA CECILIA MORA CORREA
Jefe Oficina de Control Interno

Elaboró:

Flor Alba Roncancio Gachancipa.
Auditor Oficina de Control Interno.