INFORME AUDITORÍA No. 07 DE 2023
OAGRI - SEGURIDAD DE LA INFORMACIÓN CIBERSEGURIDAD (SARSICI), INCLUYE VALIDACIÓN ACCESIBILIDAD WEB NTC 5854:2011

La OFCIN desarrolló el informe de Auditoría No.07 de 2023 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 2023, 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 vigencia 2022 y hasta el 28-02-2023 y aspectos de la NTC 5854:2011.

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 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 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 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.

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.

- 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.

- GR-NA-GU- 036 Guía de Protocolo de Seguridad de la Información y Ciberseguridad para Home Office, versión 1, aprobado el 21-08-2020.

- 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-018 Guía Evaluación de Riesgo de Seguridad de la Información y Ciberseguridad, versión 8, aprobado el 18-02-2021.

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

- IT-NA-GU-030 Guía de Gestión de Incidentes de Ciberseguridad, versión 2, aprobado el 24-08-2020.

- GR-NA-GU-023 Guía Gestión de Incidente de Seguridad de la Información, versión 7 aprobado el 14-04-2021.

- Guía Gestión de Incidentes de Seguridad de la Información, Código GR-NA-GU-023, Versión 8 del 13/Feb/2023.

- GR-NA-GU-017 Guía Borrado Seguro de la Información, versión 5, aprobado el 20-08-2020.

- GR-NA-GU-017 Guía Borrado Seguro de la Información Código GR-NA-GU-017, Versión: 006 del 13/Feb/2023.

- GR-NA-GU-015 Guía Gestión de Activos de Información, versión 5 aprobado el 20-08-2020.

- GR-NA-GU-015 Guía Gestión de Activos de Información, versión 6 aprobado el 13-02-2023.

- IT-NA-GU-025 Guía Portal Centro de Servicios, versión 6 de18-11-2020.

- IT-NA-GU-025 Guía Portal Centro de Servicios, versión 7 de 08-02-2023.

- GR-NA-GU-029 Guía Reporte General de Eventos de Riesgo, versión 4, aprobado el 17-01-2022.

- GR-NA-GU-029 Guía Reporte General de Eventos de Riesgo, versión 5, aprobado el 13-02-2023.

- Guía Gestión Seguridad en Redes, Código: IT-NA-GU-023, Versión 007 del 8/feb/2023.

- Guía Aprobación de REROS en el sistema de información, Código GR-NA-GU-037, Versión 002 del 8/Feb/2023.

- Guía de operación crear, modificar e inactivar usuarios y nombres de recursos de TI, Código: IT-NA-GU-009, versión: 015 del 8/feb/2023.

- Guía de operación generación de backups y proceso de restauración, Código IT-NA-GU-007, Versión: 013 del 8/feb/2023.

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

- Formato Matriz de Riesgo SGSI, Código GR-NA-FM-029, Versión 008 del 6/Dic/2022.

- GR-NA-FM-034 Formato Acuerdo de Confidencialidad y Política de Seguridad de la Información para la Relación Contractual, versión 6 aprobada el 29-08-2022.

- IT-NA-FM-004 Formato Adecuación y Destrucción de Información en Ambiente de pruebas, versión 14 aprobado el 26-08-2022.

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

- Matriz Gestión Informática y Tecnológica, Código: IT-NA-MZ-001, Versión 014 del 8/feb/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 23 de 2021 SARSICI.

Se revisa resultado de la última auditoría realizada a SARSICI - Informe de Auditoría No. 12 de 2022 - en el que se evidenció 1 oportunidad de mejora; la cual a la fecha de la presente auditoría se encuentra con actividades programadas con fecha de inicio 21/12/2022 y fecha de finalización a 30/06//2023, tal como se muestra en la siguiente imagen:

Figura 1 Estado PMP Auditoría SARSICI vigencia 2022
Fuente: Suite Visión Empresarial (SVE), 30/03/2023

5.2. Respuestas recibidas de la solicitud de información.

Teniendo en cuenta el requerimiento realizado el pasado 17 de marzo de 2023, a la Jefatura de OAGRI, con fecha 23-03-2023 se dispuso la información requerida en el repositorio implementado para tal efecto: OAGRICajaHonor - DOCUMENTOS AUDITORIA SARCISI 2023 - Todos los documentos (sharepoint.com), como se muestra en la siguiente imagen:

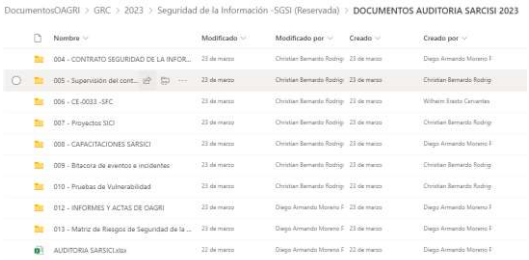


Figura 2 Archivos dispuesto por OAGRI en Repositorio Sharepoint
Fuente: Repositorio Documental Sharepoint

Asimismo, se requirió la información pertinente para el proceso de auditoría a la OAINF, quien con fecha 28-03-2023 dispuso parte de la información en el repositorio documental implementado para tal efecto:

Figura 3 Archivos dispuesto por OAINF en repositorio SharePoint
Fuente: Repositorio Documental SharePoint

Igualmente, mediante email del 28-03-2023 la OAINF remitió la siguiente información:

Figura 4 Información remitida por OAINF
Fuente: Correo electrónico Outlook.

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

Figura 5 OAGRI Relación de personal de Seguridad de la información y ciberseguridad
Fuente: Repositorio Documental SharePoint

Información reportada por OAINF

Tabla 1 Relación de personal de ciberseguridad

	RESPONSABILIDADES
	1. Análisis de vulnerabilidades de código durante el ciclo de vida de desarrollo de sistemas de información. 2. Monitoreo de las plataformas de ciberseguridad y seguridad perimetral, para proteger la infraestructura tecnológica. 3. Informar los hallazgos detectados en la aplicación y servicios web de Caja Honor. 4. Monitorear las alertas que se puedan generar de los ataques hacia Caja Honor. 5. Elaborar los temas relacionados a calidad, planes de acción y seguimiento, correspondiente a ciberseguridad.
	1. Administrar los dispositivos de ciberseguridad de la Entidad y ejecutar las acciones necesarias para su correcta operación. 2. Controlar y gestionar los documentos generados de las solicitudes que realizan los funcionarios de la Entidad para el desarrollo de sus actividades. 3. Realizar la supervisión de contratos TI, relacionados a Ciberseguridad, delegados por el jefe de la Oficina Asesora de Informática. 4. Elaborar los temas relacionados a calidad, planes de acción y seguimiento, correspondiente a ciberseguridad. 5. Ejecutar las reglas apropiadas para los dispositivos Firewall, que garanticen la correcta operación. 6. Cumplir con la normatividad vigente relacionada a las TIC y aplicable al

		RESPONSABILIDADES
		servicio a prestar. 7. Monitorear plataformas de Ciberseguridad de la Entidad, realizar afinamiento y mejoras necesarias para proteger la infraestructura tecnológica.
		1. Liderar, coordinar, gestionar y administrar las plataformas de Ciberseguridad y Seguridad Perimetral que la Entidad posee a nivel nacional. 2. Monitorear las plataformas de Ciberseguridad de Caja Honor y realizar las mejoras y ajustes necesarios a fin de que los controles aplicados sean lo más efectivos y precisos para proteger la infraestructura tecnológica. 3. Efectuar la supervisión de los proyectos T.I. asignados por la jefatura para llevar el control de la ejecución de los contratos de Ciberseguridad. 4. Liderar y Coordinar las actividades relacionadas a Ciberseguridad, con el fin de cumplir con los controles de la norma ISO 27001 y el Marco de Ciberseguridad ISO 27032. 5. Coordinar las actividades de gestión de Ciberseguridad para el Plan de Recuperación de Desastres.

Fuente: OAINF Email 28-03-2023

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 pudieran afectar la seguridad de la información en uno de sus principales pilares como lo es la confidencialidad, ya sea en reposo o en tránsito; asimismo, se conoció que OAINF cuenta con herramientas que permiten el aseguramiento de la información.

5.3.2.1. Herramientas de Monitoreo

En el proceso de revisión y entrevista con los colaboradores encargados de la Seguridad de la Información, se identificaron las siguientes herramientas para la seguridad de la Información y Ciberseguridad, tendientes a brindar seguridad fortaleciendo la infraestructura a nivel de redes y software:

Lista de herramientas suministradas por OAINF

Figura 6 Herramientas de monitoreo suministradas por OAINF
Fuente Email 28-03-2023

Lista de herramientas suministradas por OAGRI

Tabla 2 Lista de Herramientas Seguridad de la Información y Ciberseguridad

HERRAMIENTA	DESCRIPCION	EVIDENCIA

Fuente: OAGRICajaHonor - DOCUMENTOS AUDITORIA SARCISI 2023 - Todos los documentos (sharepoint.com)

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:

Figura 7 Documentos asociados a Ciberseguridad
Fuente Isolución ® 5 Consultado 20-04-2023

Seguridad de la Información

Figura 8 Documentos asociados a Seguridad de la Información
Fuente: Isolución ® 5 Consultado 20-04-2023

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:

5.3.2.2. Cronograma Escaneos

- **Cronograma de Escaneos Aplicativos Vigencia 2023**

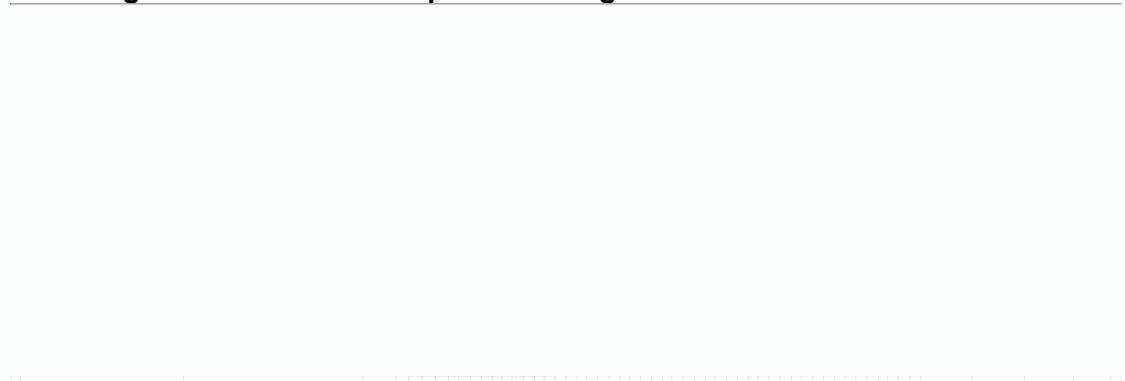


Figura 9 Cronograma Escaneo de Vulnerabilidades Aplicativos Caja Honor
Fuente: OAGRICajaHonor - Cronograma de análisis de vulnerabilidades - Todos los documentos (sharepoint.com).

- **Cronogramas Escaneos Portales Web**

Figura 10 Cronograma Escaneo de Vulnerabilidades Portales Web Caja Honor
Fuente: OAGRICajaHonor - Cronograma de análisis de vulnerabilidades - Todos los documentos (sharepoint.com)

Asimismo, se indaga con la OAGRI respecto al monitoreo sobre los portales Web de Caja Honor, para lo cual el profesional de Ciberseguridad de la firma Wexler, indica que en Caja Honor existen los siguientes 4 portales:

Tabla 3 Portales Web Caja Honor

Fuente: OAGRI - profesional de Ciberseguridad de la firma Wexler

A los cuales se les realizar monitoreo periódicamente generando un informe mensual, en donde las herramientas utilizadas para el análisis de vulnerabilidades son las citadas a continuación:

Tabla 4 URL y Herramientas de Escaneo Portales Web Caja Honor

Fuente: OAGRI - Profesional de Ciberseguridad de la firma Wexler

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 que la documentación:

Figura 11 Documentos asociados a Accesibilidad Web
Fuente: http://isolucion/IsolucionSig/Documentacion/frmListadoMaestroDocumentos.aspx, Consultado: Isolucion 20-04-2023.

5.3.2.3. Análisis de Vulnerabilidad Aplicados

La OAGRI en la vigencia 2023 realizó escaneos a la plataforma tecnológica de Caja honor mediante la tecnología de Caja Blanca en atención a que en caja negra con los controles que se tienen actualmente implementados no es posible la explotación de estas vulnerabilidades, en donde se suministraron los siguientes informes, los cuales la OFCIN procedió a analizar:

- **Herramienta Ossim de AlienVault**

Respecto a los escaneos realizados con la herramienta Ossim de AlienVault, se toma al azar el escaneo realizado con fecha 2023-03-15 23:34:45 a los diferentes sistemas de información de la Entidad, en donde dicho escaneo encontró vulnerabilidades en 11 direcciones IP correspondientes a la VLAN 172.20.0.0 / 24, así:

Figura 12 Archivo Vulnerabilidades informáticas febrero – marzo 2023
Fuente: OAGRI Email 13-04-2023

Así las cosas, se procede a revisar las vulnerabilidades de Nivel Alto encontradas sobre la IP 172.20.0.6 correspondiente a una interfaz ILO que solo tiene acceso el administrador de servidores, en donde a continuación se presenta el resumen de ellas:

Tabla 5 Vulnerabilidades_ IP 172.20.0.6 Nivel Alto_Escaneo herramienta Ossim Alien Vault

ITEM	VULNERABILIDAD	DESCRIPCION	ACCIONES

Fuente: OAGRI Email 13-04-2023 - Archivo Vulnerabilidades informáticas febrero – marzo 2023

Recomendación 1.

Dado lo anteriormente expuesto, la OFCIN recomienda a la OAINF en conjunto con OAGRI llevar a cabo la aplicación de las acciones pertinentes para remediar las vulnerabilidades relacionadas en la Tabla 5 Vulnerabilidades_ IP 172.20.0.6 Nivel Alto_Escaneo herramienta Ossim Alien Vault y suministrar las evidencias de las acciones aplicadas, a fin 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, atendiendo las buenas prácticas de seguridad de la información y los lineamientos impartidos por la ISO 27001:2013, minimizando la materialización de posibles riesgos asociados con RSI031 - Pérdida de Información, R010 - Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad; así como el incumplimiento a las Dimensiones de MIPG V5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.

Asimismo, verificar la pertinencia de la actualización del procedimiento código GR-NA-PR-028, no solo en su contenido sino en la normatividad vigente aplicable y responsables del mismo.

Fuente: OAGRI Email 13-04-2023 - Archivo Vulnerabilidades informáticas febrero – marzo 2023

5.3.2.4. Herramienta Fortify Security de Micro Focus

Acorde a la información suministrada por OAINF respecto a los análisis de vulnerabilidades llevados a cabo sobre los diferentes aplicativos utilizados en Caja Honor para su operación, durante el periodo evaluado, se extracto la siguiente información:

Figura 13 Vulnerabilidades por Nivel de Criticidad
Fuente: OAINF archivo 7.1Reporte Fenix.pdf

Asimismo, a continuación se presenta la categorización de las vulnerabilidades encontradas, acorde al reporte:

Figura 14 Categorización de Vulnerabilidades
Fuente: OAINF archivo 7.1Reporte Fenix.pdf

Figura 15 Resumen Vulnerabilidades Nivel Alto relacionadas con Integración de contraseñas dentro del código
Fuente: OAINF archivo 7.1Reporte Fenix.pdf

Figura 16 Detalle Vulnerabilidades Nivel Alto relacionadas con Integración de contraseñas dentro del código
Fuente: OAINF archivo 7.1Reporte Fenix.pdf

Figura 18 19 Detalle Vulnerabilidades Nivel Alto relacionadas con contraseñas vacías
Fuente: OAINF archivo 7.1Reporte Fenix.pdf

Figura 20 Resumen Vulnerabilidades Nivel Critico relacionadas con claves de cifrado con codificación rígida
Fuente: OAINF archivo 7.1Reporte Fenix.pdf

Figura 21 Detalle Vulnerabilidades Nivel Critico relacionadas con claves de cifrado con codificación rígida
Fuente: OAINF archivo 7.1Reporte Fenix.pdf

Figura 23 Vulnerabilidades por Nivel de Criticidad
Fuente: OAINF archivo 7.2 Reporte Fenix2.pdf

Asimismo, a continuación se presenta la categorización de las vulnerabilidades encontradas, acorde al reporte:

Figura 24 Categorización de Vulnerabilidades
Fuente: OAINF archivo 7.2 Reporte Fenix2.pdf

Figura 27 Resumen Vulnerabilidades Nivel Alto relacionadas con Gestión de contraseñas: Contraseña Vacía
Fuente: OAINF archivo 7.2 Reporte Fenix2.pdf

Figura 29 Actividad MA453240 – Service Manager – Subsanación vulnerabilidades
Fuente: OAINF – Email 20-04-2023

Figura 30 Vulnerabilidades por Nivel de Criticidad
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Asimismo, a continuación se presenta la categorización de las vulnerabilidades encontradas, según el reporte:

Figura 31 Categorización de Vulnerabilidades
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

En el ejercicio auditor se verificaron las acciones llevadas a cabo por el personal responsable de ciberseguridad de la Entidad para subsanar las vulnerabilidades encontradas frente a los hallazgos categorizados como High (Alto) y Medium (Medio) , en donde para el caso, corresponden a un Total de 12, de las cuales 8 vulnerabilidades categorizadas con Nivel Alto y 4 en Nivel Medio.

Nivel Alto:

Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Lo que no es una buena práctica dado que el almacenamiento de una contraseña de texto sin formato en un archivo de configuración puede comprometer el sistema.

Fuente: OAINF archivo 7.3 Reporte GA2.pdf

En donde, 3 de las 8 vulnerabilidades categorizadas en nivel Alto corresponden a: Categoría: Esquema XML débil, en donde los atacantes pueden aprovechar los esquemas que permiten acceso ilimitado elementos proporcionando una aplicación con una gran cantidad de elementos que hacen que la aplicación agote los recursos del sistema. A continuación se presenta el detalle de tales vulnerabilidades:

Figura 34 Resumen Vulnerabilidades Nivel Alto relacionadas con Categoría: Esquema XML débil
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Figura 35 Detalle Vulnerabilidades Nivel Alto relacionadas con Categoría: Esquema XML débil
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Figura 36 Detalle Vulnerabilidades Nivel Alto relacionadas con NegocioSN.snk.pfx
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Figura 37 Resumen Vulnerabilidades Nivel Medio relacionadas con No definición de ninguna seguridad de transporte o mensaje
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Figura 38 Detalle Vulnerabilidades Nivel Medio relacionadas con No definición de ninguna seguridad de transporte o mensaje
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Figura 39 Resumen Vulnerabilidades Nivel Medio relacionadas con Categoría: Configuración incorrecta de ASP.NET
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Figura 40 Detalle Vulnerabilidades Nivel Medio relacionadas con Categoría: Configuración incorrecta de ASP.NET
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Figura 41 Resumen Vulnerabilidades Nivel Medio relacionadas con Categoría: HTML5: MIME Sniffing
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

Figura 42 Detalle Vulnerabilidades Nivel Medio relacionadas con Categoría: HTML5: MIME Sniffing
Fuente: OAINF archivo 7.3 Reporte GA2.pdf

5.3.2.5. Herramienta Fortify Developer Workbook de Micro Focus

Mediante esta herramienta la OAINF informa que efectúo análisis de vulnerabilidades en la vigencia 2022 al sitio Web de la Entidad, así:

7.5 Reporte Web.pdf

Figura 43 Vulnerabilidades por Nivel de Criticidad
Fuente: OAINF archivo 7.5 Reporte Web.pdf

Asimismo, a continuación se presenta la categorización de las vulnerabilidades encontradas, según el reporte:

Figura 44 Categorización de Vulnerabilidades
Fuente: OAINF archivo 7.5 Reporte Web.pdf

Nivel Alto

Figura 45 Resumen Vulnerabilidades Nivel Alto Fortyfy Developer Workbook
Fuente: OAINF archivo 7.5 Reporte Web.pdf

Figura 46 Detalle Vulnerabilidades Nivel Alto login.jsf, línea 0 (Cross-Frame Scripting)
Fuente: OAINF archivo 7.5 Reporte Web.pdf

Recomendación 2.

5.3.3. 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 7 Relación de Contratos Proveedor Seguridad de la Información - OAGRI

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

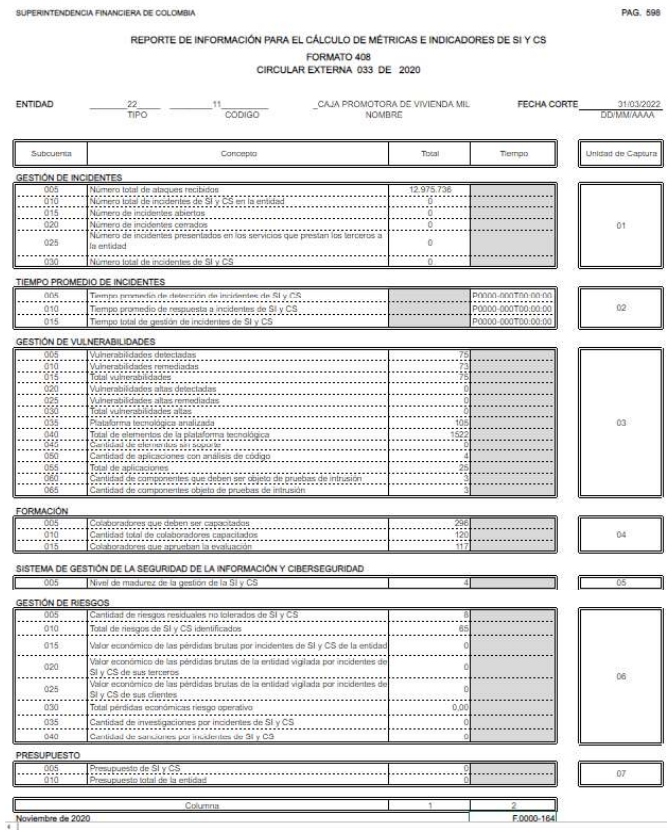
Tabla 8 Relación de Contratos Proveedor Ciberseguridad - OAINF

5.3.5.1. 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 OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com) la siguiente información que evidencia dicho trámite, correspondiente a la vigencia 2022:

Figura 49 Reporte Trimestral CE 033 de 2020 correspondiente a vigencia 2022
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

Primer Trimestre 2022



SUPERINTENDENCIA FINANCIERA DE COLOMBIA — PAG. 598

REPORTE DE INFORMACIÓN PARA EL CÁLCULO DE MÉTRICAS E INDICADORES DE SI Y CS
FORMATO 408
CIRCULAR EXTERNA 033 DE 2020

ENTIDAD 22 (TIPO) 11 (CÓDIGO) CAJA PROMOTORA DE VIVIENDA MIL (NOMBRE) FECHA CORTE 31/03/2022 (DD/MM/AAAA)

Subcuenta	Concepto	Total	Tiempo	Unidad de Captura
GESTIÓN DE INCIDENTES				
005	Número total de ataques recibidos	12.975.736		01
010	Número total de incidentes de SI y CS en la entidad	0		
015	Número de incidentes abiertos	0		
020	Número de incidentes cerrados	0		
025	Número de incidentes presentados en los servicios que prestan los terceros a la entidad	0		
030	Número total de incidentes de SI y CS	0		
TIEMPO PROMEDIO DE INCIDENTES				
005	Tiempo promedio de detección de incidentes de SI y CS		P0000.000T00.00.00	02
010	Tiempo promedio de respuesta a incidentes de SI y CS		P0000.000T00.00.00	
015	Tiempo total de gestión de incidentes de SI y CS		P0000.000T00.00.00	
GESTIÓN DE VULNERABILIDADES				
005	Vulnerabilidades detectadas	71		03
010	Vulnerabilidades remediadas	71		
015	Total vulnerabilidades	71		
020	Vulnerabilidades altas detectadas	0		
025	Vulnerabilidades altas remediadas	0		
030	Total vulnerabilidades altas	0		
035	Plataforma tecnológica analizada	60		
040	Total de elementos de la plataforma tecnológica	152		
045	Cantidad de cambios en activos de	0		
050	Cantidad de aplicaciones con análisis de código	0		
055	Total de aplicaciones	35		
060	Cantidad de componentes que deben ser objeto de pruebas de intrusión	0		
065	Cantidad de componentes objeto de pruebas de intrusión	0		
FORMACIÓN				
005	Colaboradores que deben ser capacitados	296		04
010	Cantidad total de colaboradores capacitados	121		
015	Colaboradores que aprueban la evaluación	117		
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD				
005	Nivel de madurez de la gestión de la SI y CS	4		05
GESTIÓN DE RIESGOS				
005	Cantidad de riesgos residuales no tolerados de SI y CS	8		06
010	Total de riesgos de SI y CS identificados	65		
015	Valor económico de las pérdidas brutas por incidentes de SI y CS de la entidad	0		
020	Valor económico de las pérdidas brutas de la entidad vigilada por incidentes de SI y CS de sus terceros	0		
025	Valor económico de las pérdidas brutas de la entidad vigilada por incidentes de SI y CS de sus clientes	0		
030	Total pérdidas económicas riesgo operativo	0,00		
035	Cantidad de investigaciones por incidentes de SI y CS	0		
040	Cantidad de sanciones por incidentes de SI y CS	0		
PRESUPUESTO				
005	Presupuesto de SI y CS	0		07
010	Presupuesto total de la entidad	0		
	Columna	1	2	

Noviembre de 2020 — F.0000-164

Figura 50 Reporte Primer Trimestre vigencia 2022 - CE 033 de 2020
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

Evidencia de Envío

```
ARCHIVO FIRMADO CON FIRMA CORRECTA
Observaciones:
Proceso de verificacion de firma digital ejecutado con exito.


Respuesta para Informe= 38  Fecha= 31032022:
VALIDACION DE INFORMACION CORRECTA

CODIGO DE LA ENTIDAD ..........: 22000011
TIPO DE INFORME ...............: 38 Seguridad de la Informaci□n SI y CS
FECHA DEL INFORME .............: 31032022
FECHA Y HORA DE ENVIO .........: 11042022-08:47
C.I.D.T. ......................: 2022068903-00
RESULTADO DE LA TRANSMISION ...: VALIDACION DE INFORMACION CORRECTA
```

Figura 51 Evidencias Reporte Primer Trimestre vigencia 2022 - CE 033 de 2020
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

Segundo Trimestre 2022

SUPERINTENDENCIA FINANCIERA DE COLOMBIA PAG. 598

REPORTE DE INFORMACIÓN PARA EL CÁLCULO DE MÉTRICAS E INDICADORES DE SI Y CS
FORMATO 408
CIRCULAR EXTERNA 033 DE 2020

ENTIDAD 22 (TIPO) 11 (CODIGO) CAJA PROMOTORA DE VIVIENDA MIL (NOMBRE) FECHA CORTE 30/06/2022 (DD/MM/AAAA)

Subcuenta	Concepto	Total	Tiempo	Unidad de Captura
GESTIÓN DE INCIDENTES				
005	Número total de ataques recibidos	18,045,147		01
010	Número total de incidentes de SI y CS en la entidad	12		
015	Número de incidentes abiertos	0		
020	Número de incidentes cerrados	0		
025	Número de incidentes presentados en los servicios que prestan los terceros a la entidad	0		
030	Número total de incidentes de SI y CS	0		
TIEMPO PROMEDIO DE INCIDENTES				
005	Tiempo promedio de detección de incidentes de SI y CS		P0000-000T00:00:00	02
010	Tiempo promedio de respuesta a incidentes de SI y CS		P0000-000T00:00:00	
015	Tiempo total de gestión de incidentes de SI y CS		P0000-000T00:00:00	
GESTIÓN DE VULNERABILIDADES				
005	Vulnerabilidades detectadas	167		03
010	Vulnerabilidades remediadas	167		
015	Total vulnerabilidades	167		
020	Vulnerabilidades altas detectadas	0		
025	Vulnerabilidades altas remediadas	0		
030	Total vulnerabilidades altas	0		
035	Plataforma tecnológica analizada	178		
040	Total de elementos de la plataforma tecnológica	5,755		
045	Cantidad de elementos sin soporte	0		
050	Cantidad de aplicaciones con análisis de código	0		
055	Total de aplicaciones	31		
060	Cantidad de componentes que deben ser objeto de pruebas de intrusión	1		
065	Cantidad de componentes objeto de pruebas de intrusión	3		
FORMACIÓN				
005	Colaboradores que deben ser capacitados	303		04
010	Cantidad total de colaboradores capacitados	157		
015	Colaboradores que aprueban la evaluación	150		
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD				
005	Nivel de madurez de la gestión de la SI y CS	4		05
GESTIÓN DE RIESGOS				
005	Cantidad de riesgos residuales no tolerados de SI y CS	8		06
010	Total de riesgos de SI y CS identificados	65		
015	Valor económico de las pérdidas brutas por incidentes de SI y CS de la entidad	0		
020	Valor económico de las pérdidas brutas de la entidad vigilada por incidentes de SI y CS de sus terceros	0		
025	Valor económico de las pérdidas brutas de la entidad vigilada por incidentes de SI y CS de sus clientes	0		
030	Total pérdidas económicas riesgo operativo	141,985,132.67		
035	Cantidad de investigaciones por incidentes de SI y CS	0		
040	Cantidad de sanciones por incidentes de SI y CS	0		
PRESUPUESTO				
005	Presupuesto de SI y CS	0		07
010	Presupuesto total de la entidad	0		
	Columna	1	2	

Noviembre de 2020 F.0000-164

Figura 52 Reporte Segundo Trimestre vigencia 2022 - CE 033 de 2020
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

Evidencia de Envío

```
ARCHIVO FIRMADO CON FIRMA CORRECTA
Observaciones:
Proceso de verificacion de firma digital ejecutado con exito.


Respuesta para Informe= 38  Fecha= 30062022:
VALIDACION DE INFORMACION CORRECTA


CODIGO DE LA ENTIDAD ..........: 22000011
TIPO DE INFORME ..............: 39 Seguridad de la Información
SI y CS
FECHA DEL INFORME ............: 30062022
FECHA Y HORA DE ENVIO .........: 15072022-10:08
C.I.D.T. ......................: 2022136242-00
RESULTADO DE LA TRANSMISION ...: VALIDACION DE INFORMACION
CORRECTA
```

Figura 53 Evidencia Reporte Segundo Trimestre vigencia 2022 - CE 033 de 2020
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

Tercer Trimestre 2022

SUPERINTENDENCIA FINANCIERA DE COLOMBIA PAG. 598

REPORTE DE INFORMACIÓN PARA EL CÁLCULO DE MÉTRICAS E INDICADORES DE SI Y CS
FORMATO 408
CIRCULAR EXTERNA 033 DE 2020

ENTIDAD 22 (TIPO) 11 (CODIGO) _CAJA PROMOTORA DE VIVIENDA MIL (NOMBRE) FECHA CORTE 30/09/2022 (DD/MM/AAAA)

Subcuenta	Concepto	Total	Tiempo	Unidad de Captura
GESTIÓN DE INCIDENTES				
005	Número total de ataques recibidos	15'308926		01
010	Número total de incidentes de SI y CS en la entidad	0		
015	Número de incidentes abiertos	0		
020	Número de incidentes cerrados	0		
025	Número de incidentes presentados en los servicios que prestan los terceros a la entidad	0		
030	Número total de incidentes de SI y CS	0		
TIEMPO PROMEDIO DE INCIDENTES				
005	Tiempo promedio de detección de incidentes de SI y CS		P0000-000T00:00:00	02
010	Tiempo promedio de respuesta a incidentes de SI y CS		P0000-000T00:00:00	
015	Tiempo total de gestión de incidentes de SI y CS		P0000-000T00:00:00	
GESTIÓN DE VULNERABILIDADES				
005	Vulnerabilidades detectadas	153		03
010	Vulnerabilidades remediadas	153		
015	Total vulnerabilidades	153		
020	Vulnerabilidades altas detectadas	0		
025	Vulnerabilidades altas remediadas	0		
030	Total vulnerabilidades altas	0		
035	Plataforma tecnológica analizada	105		
040	Total de elementos de la plataforma tecnológica	3840		
045	Cantidad de elementos en soporte	0		
050	Cantidad de aplicaciones con análisis de código	0		
055	Total de aplicaciones	31		
060	Cantidad de componentes que deben ser objeto de pruebas de intrusión	2		
065	Cantidad de componentes objeto de pruebas de intrusión	0		
FORMACIÓN				
005	Colaboradores que deben ser capacitados	378		04
010	Cantidad total de colaboradores capacitados	135		
015	Colaboradores que aprueban la evaluación	135		
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD				
005	Nivel de madurez de la gestión de la SI y CS	4		05
GESTIÓN DE RIESGOS				
005	Cantidad de riesgos residuales no tolerados de SI y CS	0		06
010	Total de riesgos de SI y CS identificados	85		
015	Valor económico de las pérdidas brutas por incidentes de SI y CS de la entidad	0		
020	Valor económico de las pérdidas brutas de la entidad vigilada por incidentes de SI y CS de sus terceros	0		
025	Valor económico de las pérdidas brutas de la entidad vigilada por incidentes de SI y CS de sus clientes	0		
030	Total pérdidas económicas riesgo operativo	8.719.072,50		
035	Cantidad de investigaciones por incidentes de SI y CS	0		
040	Cantidad de sanciones por incidentes de SI y CS	0		
PRESUPUESTO				
005	Presupuesto de SI y CS	0		07
010	Presupuesto total de la entidad	0		
	Columna	1	2	

Noviembre de 2020 F-0000-164

Figura 54 Reporte Tercer Trimestre vigencia 2022 - CE 033 de 2020
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

Evidencia de Envío

```
ARCHIVO FIRMADO CON FIRMA CORRECTA
Observaciones:
Proceso de verificacion de firma digital ejecutado con exito.


Respuesta para Informe= 38  Fecha= 30092022:
VALIDACION DE INFORMACION CORRECTA

♠CODIGO DE LA ENTIDAD ..........: 22000011
TIPO DE INFORME ................: 38 Seguridad de la Informaci♠n SI y CS
FECHA DEL INFORME ..............: 30092022
FECHA Y HORA DE ENVIO ..........: 13102022-11:15
C.I.D.T. .......................: 2022199326-00
RESULTADO DE LA TRANSMISION ...: VALIDACION DE INFORMACION CORRECTA
```

Figura 55 Evidencia reporte Tercer Trimestre vigencia 2022 - CE 033 de 2020
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

Cuarto Trimestre 2022

SUPERINTENDENCIA FINANCIERA DE COLOMBIA PAG. 598

REPORTE DE INFORMACIÓN PARA EL CÁLCULO DE MÉTRICAS E INDICADORES DE SI Y CS

FORMATO 408

CIRCULAR EXTERNA 033 DE 2020

ENTIDAD 22 (TIPO) 11 (CODIGO) CAJA PROMOTORA DE VIVIENDA MIL (NOMBRE) FECHA CORTE 31/12/2022 (DD/MM/AAAA)

Subcuenta	Concepto	Total	Tiempo	Unidad de Captura
GESTIÓN DE INCIDENTES				
005	Número total de ataques recibidos	4.065.159		01
010	Número total de incidentes de SI y CS en la entidad	0		
015	Número de incidentes abiertos	0		
020	Número de incidentes cerrados	0		
025	Número de incidentes presentados en los servicios que prestan los terceros a la entidad	0		
030	Número total de incidentes de SI y CS	0		
TIEMPO PROMEDIO DE INCIDENTES				
005	Tiempo promedio de detección de incidentes de SI y CS		P0000-000T00:00:00	02
010	Tiempo promedio de respuesta a incidentes de SI y CS		P0000-000T00:00:00	
015	Tiempo total de gestión de incidentes de SI y CS		P0000-000T00:00:00	
GESTIÓN DE VULNERABILIDADES				
005	Vulnerabilidades detectadas	0		03
010	Vulnerabilidades remediadas	0		
015	Total vulnerabilidades	0		
020	Vulnerabilidades altas detectadas	0		
025	Vulnerabilidades altas remediadas	0		
030	Total vulnerabilidades altas	0		
035	Plataforma tecnológica analizada	128		
040	Total de elementos de la plataforma tecnológica	3840		
045	Cantidad de elementos sin soporte	0		
050	Cantidad de aplicaciones con análisis de código	7		
055	Total de aplicaciones	31		
060	Cantidad de componentes que deben ser objeto de pruebas de intrusión	4		
065	Cantidad de componentes objeto de pruebas de intrusión	4		
FORMACIÓN				
005	Colaboradores que deben ser capacitados	53		04
010	Cantidad total de colaboradores capacitados	53		
015	Colaboradores que aprueban la evaluación	53		
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD				
005	Nivel de madurez de la gestión de la SI y CS	4		05
GESTIÓN DE RIESGOS				
005	Cantidad de riesgos residuales no tolerados de SI y CS	0		06
010	Total de riesgos de SI y CS identificados	65		
015	Valor económico de las pérdidas brutas por incidentes de SI y CS de la entidad	0		
020	Valor económico de las pérdidas brutas de la entidad vigilada por incidentes de SI y CS de sus terceros	0		
025	Valor económico de las pérdidas brutas de la entidad vigilada por incidentes de SI y CS de sus clientes	0		
030	Total pérdidas económicas riesgo operativo	324.654.092,93		
035	Cantidad de investigaciones por incidentes de SI y CS	0		
040	Cantidad de sanciones por incidentes de SI y CS	0		
PRESUPUESTO				
005	Presupuesto de SI y CS	0		07
010	Presupuesto total de la entidad	0		
	Columna	1	2	

Noviembre de 2020 F.0000-164

Figura 56 Reporte Cuarto Trimestre vigencia 2022 - CE 033 de 2020
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

Evidencia de Envío

```
ARCHIVO FIRMADO CON FIRMA CORRECTA
Observaciones:
Proceso de verificacion de firma digital ejecutado con exito.


Respuesta para Informe= 38  Fecha= 31122022:
VALIDACION DE INFORMACION CORRECTA

CODIGO DE LA ENTIDAD ..........: 22000011
TIPO DE INFORME ...............: 38 Seguridad de la Informaci□n SI y CS
FECHA DEL INFORME .............: 31122022
FECHA Y HORA DE ENVIO .........: 13012023-14:40
C.I.D.T. ......................: 2023008965-01
RESULTADO DE LA TRANSMISION ...: VALIDACION DE INFORMACION CORRECTA
```

Figura 57 Evidencia Reporte Cuarto Trimestre vigencia 2022 - CE 033 de 2020
Fuente OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

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.

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

Fuente: AUDITORIA SARSICI - 5) Proyectos Ciberseguridad - Todos los documentos (sharepoint.com)

Tabla 9 Relación de Proyectos Ciberseguridad

Igualmente, la OAGRI suministra información relacionada en los siguientes archivos:

Figura 59 OAGRI Proyectos Ciberseguridad
Fuente: OAGRICajaHonor - 007 - Proyectos SICI - Todos los documentos (sharepoint.com)

No obstante, la OFCIN al revisar la información contenida en ellos evidencia que dicha información corresponde a capacitaciones, socialización, pruebas de ingeniería social ejecutadas por la OAGRI y el proveedor Wexler, tendientes a socializar con los colaboradores de la Entidad información relevante que permita permanecer alerta frente a diferentes eventos sospechosos

que puedan llegar a comprometer la seguridad de la información de Caja Honor. Así las cosas, la información de este ítem será presentada en el ítem de capacitaciones y pruebas de ingeniería social.

5.3.7. **Reporte de capacitaciones al personal**

La OAGRI mediante el repositorio documental dispuso información concerniente a las capacitaciones y pruebas de ingeniería efectuadas en la vigencia 2022, como se muestra en la siguiente tabla:

Tabla 10 Capacitación y Pruebas de Ingeniería Social

Fuente: OAGRICajaHonor - SEGURIDAD DE LA INFORMACION - Todos los documentos (sharepoint.com)

Asimismo la OAGRI y el proveedor Wexler llevaron a cabo capacitaciones de Seguridad de la Información y ciberseguridad correspondientes a la vigencia 2022, tales como:

VIGENCIA 2022

CAPACITACIONES I TRIMESTRE

Mes	Funcionarios	Contratistas /Outsourcing	Aprendices / Practicantes	Enlaces	TOTAL
Enero	23	0	0	0	23
Febrero	21	0	0	0	21
Marzo	80	42	0	0	122
TOTAL	124	42	0	0	166

CAPACITACIONES II TRIMESTRE

Mes	Funcionarios	Contratistas /Outsourcing	Aprendices / Practicantes	Enlaces	TOTAL
Abril	0	0	0	0	0
Mayo	0	0	0	0	0
Junio	0	23	0	0	23
TOTAL	0	23	0	0	23

CAPACITACIONES III TRIMESTRE

Mes	Funcionarios	Contratistas /Outsourcing	Aprendices / Practicantes	Enlaces	TOTAL
Julio					0
Agosto	51	0	0		51
Septiembre	71	3	0		74
TOTAL	122	3	0	0	125

CAPACITACIONES IV TRIMESTRE

Mes	Funcionarios	Contratistas /Outsourcing	Aprendices / Practicantes	Enlaces	TOTAL
Noviembre	190	22			212
Diciembre	185	4			189
TOTAL	375	26	0	0	401

Figura 60 Capacitaciones Seguridad de la Información vigencia 2022
Fuente OAGRI OAGRICajaHonor - 008 - CAPACITACIONES SARSICI - Todos los documentos (sharepoint.com)

Cuyas evidencias del personal asistente se pueden observar en el siguiente link: Consolidad Capacitación SICI 2022.xlsx

Inducción

INDUCCIONES I TRIMESTRE					
Mes	Funcionarios	atistas /Outsou	dices / Practi	Enlaces	TOTAL
Enero	2	2	2	2	8
Febrero	23	6	0	0	29
Marzo	0	5	1	0	6
TOTAL	25	13	3	2	43

INDUCCIONES II TRIMESTRE					
Mes	Funcionarios	atistas /Outsou	dices / Practi	Enlaces	TOTAL
Abril	1	3	6		10
Mayo					
Junio					
TOTAL	1	3	6	0	10

INDUCCIONES III TRIMESTRE					
Mes	Funcionarios	Contratistas /Outsourcing	Aprendices /	Enlaces	TOTAL
Julio	0	0	0	0	0
Agosto	67	10	1	4	82
Septiembre	10	0	2	0	12
TOTAL	77	10	3	4	94

INDUCCIONES IV TRIMESTRE					
Mes	Funcionarios	atistas /Outsou	dices / Practi	Enlaces	TOTAL
Octubre					-
Noviembre					-
Diciembre					-
TOTAL	0	0	0	0	0

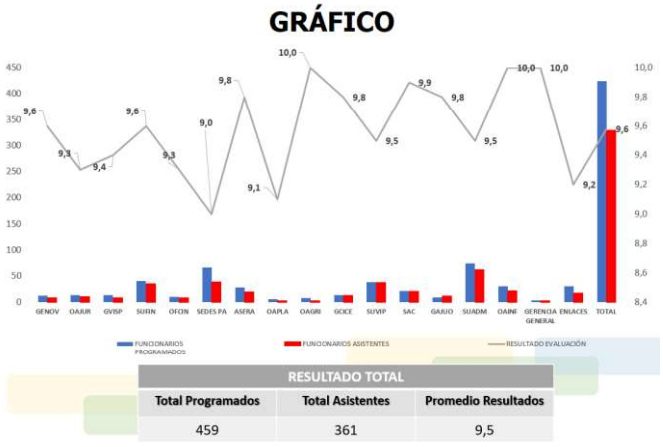
CCIONES SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGUR					
Mes	Funcionarios	atistas /Outsou	dices / Practi	Enlaces	TOTAL
Agosto	19	1	1	4	25
Septiembre	9	1	2		12
TOTAL	28	2	3	4	37

Figura 61 Proceso de Inducciones vigencia 2022
Fuente OAGRI OAGRICajaHonor - 008 - CAPACITACIONES SARSICI - Todos los documentos (sharepoint.com)

Consolidado
Inducción SICI 2022.

VIGENCIA 2023

Durante el mes de enero de 2023, la OAGRI llevó a cabo capacitaciones sobre CAPACITACIÓN SI-CI 2023 a los funcionarios de la Entidad en donde se tenía programado un total de 459 colaboradores de los cuales asistieron 361, como se muestra en el siguiente gráfico:



RESULTADO TOTAL		
Total Programados	Total Asistentes	Promedio Resultados
459	361	9,5

El detalle del personal asistente y ausente, así como las evidencias del control de la asistencia a las citadas capacitaciones y evaluaciones aplicadas tendientes a conocer el nivel de conocimientos adquiridos, se puede observar en el siguiente enlace: 1 Enero

Inducciones

A continuación se presenta la lista del personal que recibieron inducción por parte de la OAGRI durante el mes de febrero de 2023:

Figura 62 Inducciones vigencia 2023
Fuente OAGRI OAGRICajaHonor - 008 - CAPACITACIONES SARSICI - Todos los documentos (sharepoint.com)

Reinducción

A continuación se presenta la lista del personal que recibieron reinducción por parte de la OAGRI durante el mes de febrero de 2023, en relación con temas de Seguridad de la Información e Incumplimiento de Políticas:

Figura 63 Reinducciones vigencia 2023
Fuente OAGRI OAGRICajaHonor - 008 - CAPACITACIONES SARSICI - Todos los documentos (sharepoint.com)

5.3.8. Reportes de eventos e incidente Seguridad de la Información y Ciberseguridad

Se informa por parte de OAGRI que en la vigencia 2022 los reportes de eventos / Incidentes se llevaba control manual en Excel.

BITACORA DE EVENTOS E INCIDENTES 2022.xlsx

Para la vigencia 2023, la OAGRI informa que se implementó el reporte de eventos / Incidentes a través del Centro de Servicios, como se muestra a continuación:

Fuente: OAGRI Vía Team – Consultado 18-04-2023

En prueba de recorrido con el consultor de seguridad de la información de OAGRI, la OFCIN requirió generar el reporte correspondiente al primer trimestre de 2023, observando que al ingresar a la herramienta y seleccionar la opción “Solicitudes OAGRI” se presenta de forma general el listado de Incidentes y Eventos registrados por los diferentes colaboradores de la Entidad, desde la fecha de implementación de la herramienta hasta la fecha actual; es decir la herramienta no contempla un reporte que permita indicar un periodo de tiempo dado y genere de forma automática la información requerida. Entre tanto, para obtener la información correspondiente al primer trimestre de la vigencia 2023, fue necesario seleccionar todos los datos de la Consola del Centro de Servicios y con la opción copiar llevarlos a un archivo Excel, observando además que no se cuenta con la información relacionada con la respuesta o solución del incidente o evento, por lo que de forma manual, se debe abrir uno a uno los SR o identificación del registro de Incidente o Evento y complementar en una columna del archivo Excel dicha información.

Así las cosas, para el Primer Trimestre de 2023 la OAGRI suministró un total de 20 registros de los cuales 18 presentan estado “Cerrado” y los 2 restantes presentan estado “Enviado”, es decir que no han sido concluidos, así:

Tabla 11 Reporte de Incidentes y Eventos de Seguridad Primer Trimestre 2023

Estado	Titulo	Cant.
Cerrado	0	1
	Incidentes y eventos para la OAGRI. verificar la información en la "Entrada del usuario".	17
Enviado	Incidentes y eventos para la OAGRI. verificar la información en la "Entrada del usuario".	2
Total general		**20**

Fuente: OAGRI - 009 Incidentes - Eventos Corte Abril 2023.xlsx (sharepoint.com)

Asimismo, se observa que no se identifica si el registro corresponde a Evento o a Incidente puesto que el Título es el mismo para todos; además de encontrarse un registro sin información en el título.

El detalle de dichos registros de información se pueden observar en el siguiente archivo:

009 Incidentes - Eventos Corte Abril ;

Por lo anteriormente expuesto, y teniendo en cuenta que la herramienta Centro de Servicios no cuenta con un reporte de eventos / incidentes registrados en dicha plataforma, por lo que el reporte debe construirse de forma manual, copiando los datos en una hoja de Excel y adicionando la información relacionada con la solución o acciones ejecutadas frente al tema para la subsanación, en donde el margen de error tiende a aumentar, además de que se puede presentar posible manipulación de los datos, la OFCIN recomienda:

Oportunidad de Mejora Correctiva 1.

En la prueba de recorrido con el consultor de seguridad de OAGRI, se evidenció que para obtener la información de Eventos / Incidentes correspondiente al primer trimestre de la vigencia 2023, fue necesario hacerlo manualmente, seleccionando todos los datos de la Consola del Centro de Servicios y con la opción copiar llevarlos a un archivo Excel, observando además que no se cuenta con la información relacionada con la respuesta o solución del incidente o evento, la cual se debió complementar igualmente de forma manual; por lo tanto, la OFCIN recomienda a la OAGRI, estudiar la posibilidad con el proveedor de la herramienta Centro de Servicios, la creación e implementación de una opción de reportes automáticos de Eventos / Incidentes registrados en un periodo dado, tendiente a optimizar el proceso y a preservar los pilares fundamentales de seguridad de la información indicados por el Estándar ISO:27001:2013 como son la Integridad, Confidencialidad y Disponibilidad, dando cumplimiento a lo establecido en el ítem A12 del Anexo A del citado Estándar y a las buenas prácticas aplicables al manejo de la información; GR-NA-MA-009 Manual Seguridad de la Información y Ciberseguridad, versión 3, aprobado el 25-06-2021, de tal forma que se minimice la materialización de posibles riesgos asociados RSI030 – Información Errada, RSI036 – Pérdida de Confidencialidad del Activo de Información, así como el cumplimiento a las Dimensiones de MIPG Versión 5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.

5.3.9. 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

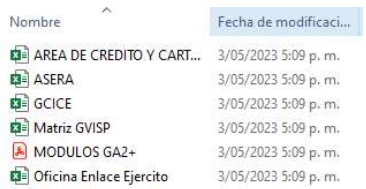
usuarios alineados con la Matriz de Segregación de Funciones, es decir acorde a las actividades asignadas en el desempeño de sus funciones.

Teniendo en cuenta que tanto en la acción de mejora No. 408 aperturada el 24-06-2022 producto de la Auditoría Interna de Calidad de la Norma ISO 27001:2013, como en la acción de mejora OMP1. OAGRI aperturada con fecha 21/12/2022 producto del ejercicio auditor No. 12 de 2022 OAGRI - Seguridad de la Información Ciberseguridad (SARSICI), incluye validación Accesibilidad Web NTC 5854:2011 – Recomendación Furag 2021 se hace referencia a la ausencia de la Matriz de Roles/Perfiles y Permisos para las herramientas tecnológicas utilizadas en Caja Honor para su operación, es de alta prioridad su implementación 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.

Figura 65 Oportunidad de Mejora 408 – OAGRI de 24-06-2022
Fuente: Herramienta Isolucion – Auditorías Internas SGI - ISO 27001:2013

Figura 66 Oportunidad de Mejora OMP1 – OAGRI de 24-12-2022
Fuente: Herramienta SVE – Plan de Mejoramiento por Proceso - https://vision/suiteve/base/client?soa=6&_sveVrs=9650202210018

Por otra parte, en reunión de socialización del presente informe de auditoría, el líder de la OAGRI manifestó contar con avances respecto a la documentación de las matrices de Roles, Perfiles y Permisos de las diferentes herramientas tecnológicas utilizadas en Caja Honor para su operación; para lo cual, mediante email del 03-05-2023, la OAGRI suministró la siguiente información:



Que da cuenta de los avances alcanzados a la fecha frente a la documentación de matrices de Roles, Perfiles y Permisos del nuevo core del Negocio KRITERION, para las dependencias: Área Crédito y Cartera, ASERA, GAVIA, GGASE, GVISP, GCICE y OEJER. Igualmente, se informa por parte de OAGRI que la documentación de las citadas matrices, se llevó a cabo con base en el documento descriptivo de módulos y submódulos que contiene la herramienta, el cual fue suministrado por el proveedor del software. Así las cosas, la OAGRI llevó a cabo mesas de trabajo con el líder de cada uno de los procesos antes citados, quien indicó las funciones desarrolladas por cada uno de los miembros del equipo y en el formato previamente diseñado por OAGRI se documentaron los roles, perfiles y permisos a que tendrán accesos los colaboradores dentro de herramienta tecnológica.

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

Una vez analizada la información suministrada por OAGRI en el archivo usuarios_al 28022023_validado.xlsx, se observan inconsistencias tales como:

- Colaboradores que ya no prestan sus servicios en la Entidad y sin embargo el estado de su usuario en el AD se encuentra ACTIVO:

Dado lo anteriormente expuesto, se evidencia que no existe concordancia con lo descrito en la Guía de Operación Crear, Modificar e Inactivar Usuarios y Nombres de Recursos de TI, Código IT-NA-GU-009, V15 de Fecha 8/Feb/2023, **Numeral 7 "**Las cuentas de dominio de la Caja Promotora de Vivienda Militar y de Policía, así como los usuarios de los aplicativos deben ser desactivadas luego de cinco días calendario transcurridos desde el último inicio de sesión. Esta política aplica para todos los colaboradores y funcionarios de la Entidad (personal de planta y contratistas)**" y numeral 8 "** Se realizará inactivación definitiva de aquellos usuarios que lleven más de 90 días sin hacer uso de los recursos y servicios IT que les hayan sido asignados, salvo aquellos usuarios que por situaciones especiales deben permanecer activos o aquellos que han sido definidos para que funcionen adecuadamente los sistemas".

Oportunidad de Mejora Correctiva 2.

La OFCIN recomienda a la OAINF implementar y mantener un control estricto respecto a la gestión de usuarios de los servicios tecnológicos alineado con las políticas de seguridad de la información establecidas al interior de la Entidad, puesto que situaciones relacionadas con usuarios que nunca se han logueado, que su último inicio de sesión ha superado los cinco días calendario, usuarios que ya no prestan sus servicios en la Entidad y continúan con el usuario

Activo, entre otros, tal como se refiere en el numeral 5.3.9. del presente informe; no corresponden a una buena práctica de seguridad de la información, ni a lo descrito en la Guía de Operación Crear, Modificar e Inactivar Usuarios y Nombres de Recursos de TI, Código IT-NA-GU-009, V15 de Fecha 8/Feb/2023, ni da cumplimiento a lo requerido por el Estándar ISO 27001:2013, Numeral A9 del Anexo A "Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios", ni preserva los pilares fundamentales de Seguridad de la Información como son integridad, confidencialidad y disponibilidad de la misma, conllevando a la posible materialización de riesgos relacionados con RSI031 - Pérdida de Información, RSI030 – Información Errada, R010 - Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad; así como el incumplimiento a las Dimensiones de MIPG V5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.

Por otra parte, la OFCIN recomienda a la OAINF (Mesa de Ayuda) buscar los mecanismos que permitan registrar en el AD los datos principales de los colaboradores de la Entidad, tales como identificación correcta, nombres y apellidos y proceso o área al que corresponden; de tal forma que al generar el reporte se cargue dicha información principal y no se tengan que realizar procesos manuales como complementar en Excel el número de identificación de los usuarios.

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

La OAINF suministró archivo 10. PETI.pdf el cual corresponde al Plan Estratégico de Tecnología de Información 2019 -2022, en donde se encuentran documentadas las iniciativas y proyectos tecnológicos en un mapa de ruta priorizado a 4 años. No obstante, teniendo en cuenta que el periodo de vigencia de dicho plan ya finalizó al cierre de la vigencia 2022, es pertinente que 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.

5.3.11. Bitácora de Backups / Restore

La OAINF suministró los siguientes archivos correspondientes a evidencias de ejecución de backups y procesos de restauración efectuados:

BITÁCORA BACKPUS ejec AUDIT_CTRL_INT año 2023: Contiene información del Primer Trimestre de la vigencia 2023 indicando datos tales como: Nombre de la BD, Descripción del Estado, Tipo de backup y fecha de finalización del backup.

BITÁCORA AUDIT_CTRL_INT RESTAURACIÓN 2023: Se observan únicamente procesos de restauración correspondientes a periodos de tiempo 13, 21, 23 y 27 de marzo de 2023, en donde para Isolucion- Base de datos y GA2- Máquina Virtual se indica que el proceso fue completado con errores.

Acorde a la Guía de Operación Generación de Backups y Proceso de Restauración, Código IT-NA-GU-007, V13 del 08-Feb-2023 se menciona que: “Se deben realizar pruebas de restauración de los medios que se encuentran en custodia del proveedor seleccionado para tal fin por lo menos **una vez trimestral**, con el objetivo de comprobar su integridad física y lógica. Dichas pruebas pueden ser realizadas tomando muestras aleatorias. Como pruebas servirán toda restauración de copias de seguridad que se realice incluso a partir de solicitud de la realización de las mismas”, no obstante, la OAINF no suministró evidencias de pruebas de restauración realizadas para el total del periodo evaluado. Por lo anterior la OFCIN realiza la siguiente recomendación:

Recomendación 3.

Teniendo en cuenta las políticas establecidas en Caja Honor para la ejecución del proceso de restauración es importante que la OAINF desarrolle dicho proceso con la periodicidad indicada, realizando las pruebas pertinentes para verificar la funcionalidad e integridad física y lógica que garanticen el correcto funcionamiento de las copias de seguridad. Lo anterior, con el propósito de proteger y ayudar a la Entidad a recuperarse en caso de presentarse algún evento no planificado como fallos en el hardware o software, o causados por un ser humano como la eliminación accidental de datos, ataques maliciosos (virus o malware), que conlleven a la posible pérdida de información. Además de suministrar la completitud de la información correspondiente al periodo evaluado, que permita a la OFCIN realizar los análisis de información pertinente en aras de emitir las recomendaciones a que haya lugar para apoyar el mejoramiento continuo del proceso; atendiendo las buenas prácticas de seguridad de la información, Guía de Operación Generación de Backups y Proceso de Restauración, Código IT-NA-GU-007, V13 del 08-Feb-2023, además de lo descrito en el numeral A.12.3.1 del Anexo A del Estándar ISO 27001:2013 en aras de minimizar la materialización de los riesgos asociados con R035 - Deficiencia en la Calidad y Entrega Inoportuna de la Información Requerida , RSI031 - Pérdida de Información, RSI030 – Información Errada, R010 - Incumplimiento de Obligaciones Legales y/o Normativas

Aplicables a la Entidad; así como el incumplimiento a las Dimensiones de MIPG V5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.

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

Vigencia 2022

Al respecto la OAGRI suministró los siguientes archivos correspondientes a los cuatro trimestres de la vigencia 2022, con sus respectivas actas de los Comités de Riesgos 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 el correcto funcionamiento del SGSI en la Entidad y generar 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:

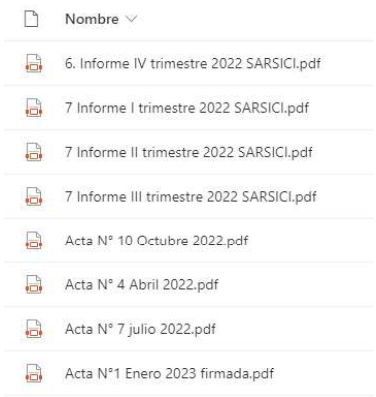


Figura 67 Informes y actas Gestión de Seguridad de la Información y Ciberseguridad
Fuente: OAGRI Repositorio Documental: OAGRICajaHonor - 2022 - Todos los documentos (sharepoint.com)

5.3.13. Inventario de Hardware (Equipos de Cómputo)

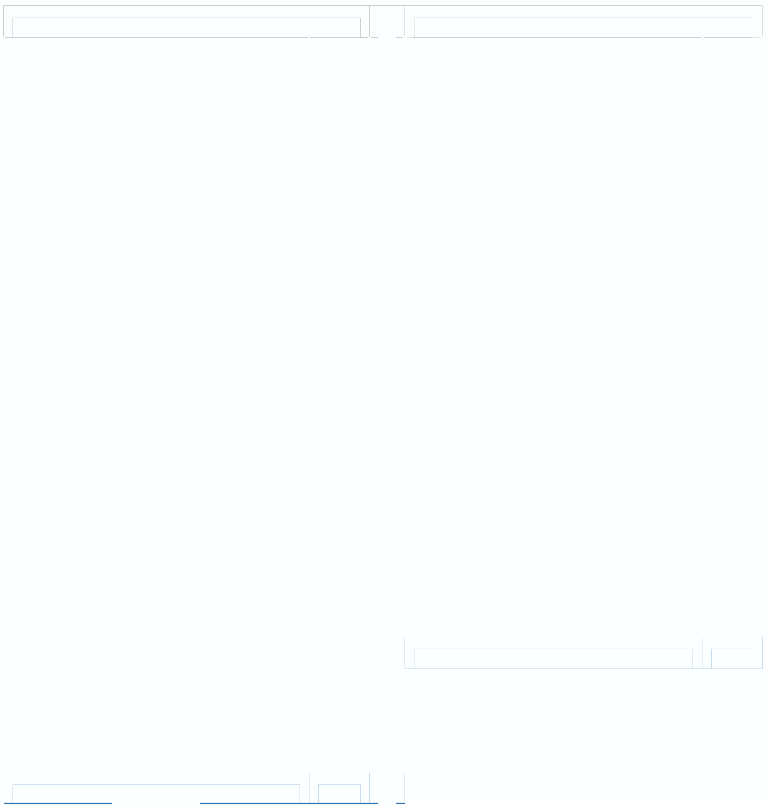
Mediante el archivo Equipos de Cómputo a Corte de Febrero 2023.xlsx la OAINF suministró el siguiente listado de equipos de cómputo con un total de 931 máquinas, distribuidas en las siguientes áreas:

Tabla 13 Relación de Equipos de Cómputo Caja Honor por dependencia

PROCESO / AREA	CANT.
DOCUMENTAL Y PREVENCIÓN	16

Fuente: OAINF - archivo EQUIPOS DE COMPUTO A CORTE DE FEBRERO 2023.xlsx

Del total (...os
de escrit(



Fuente: OAINF - archivo Equipos de Cómputo a Corte de Febrero 2023.xlsx

6. ACCESIBILIDAD WEB

Mediante email del 17-03-2023 la OFCIN requirió a OAINF el suministro de información relacionada con: “Respecto a Accesibilidad Web, favor indicar: WebMaster o responsable de la administración del sitio Web, administración de contenido, Documento que dé cuenta de la identificación, gestión, clasificación, organización y conservación de los contenidos publicados y del control de cambios de las Actualizaciones/Modificaciones aplicadas” y en respuesta a dicha petición la OAINF mediante email del 28-03-2023 informó que el responsable de dicha información es el Área de Comunicaciones, para lo cual la OFCIN procedió a solicitar a ARCOM mediante email del 12-04-2023 dicha información, en donde la líder del proceso suministra a través de correo electrónico del 14-04-2023, la siguiente información:

Figura 68 Correo electrónico con relación a Sitio Web Caja Honor
Fuente: ARCOM – Email 14-04-2023

Como se observa en la respuesta del área de Comunicaciones, no se indica quien es el WebMaster o responsable de la administración del sitio Web ni de la administración de contenido.

No obstante, al 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.

Al revisar la información contenida en el archivo Documento Esquema de Publicación Caja Honor.pdf, se observa que corresponde al esquema de publicación de la Entidad con fecha de corte al mes de agosto de la vigencia 2022, el cual contiene datos relacionados con el Nombre de la información, Descripción, Idioma, Formato, Fecha de Generación de la Información, Frecuencia de Actualización, lugar de consulta, nombre del responsable de la producción de la información y Nombre del Responsable de la Información. El detalle de dicha información se puede observar en el siguiente archivo:

esquema-publicaci
on-Caja-Honor.pdf

Asimismo, al verificar el archivo Revisión Contenidos - 2022 – 2023 se observan 189 registros correspondientes a solicitudes de publicaciones efectuadas por los diferentes procesos de la Entidad durante las vigencias 2022 y 2023, así:

		Publicaciones
		19
		2
		4
		7
		5
		1
		8
		9
		2
		7
		10
		4
		3
		2
		5
		1
		17
		11
		11
		2
		6
		10
		9
		10
		9
		13
		1
		1
Total general		189

Fuente: ARCOM – Email 14-04-2023 Archivo Revisión Contenidos - 2022 – 2023.xlsx

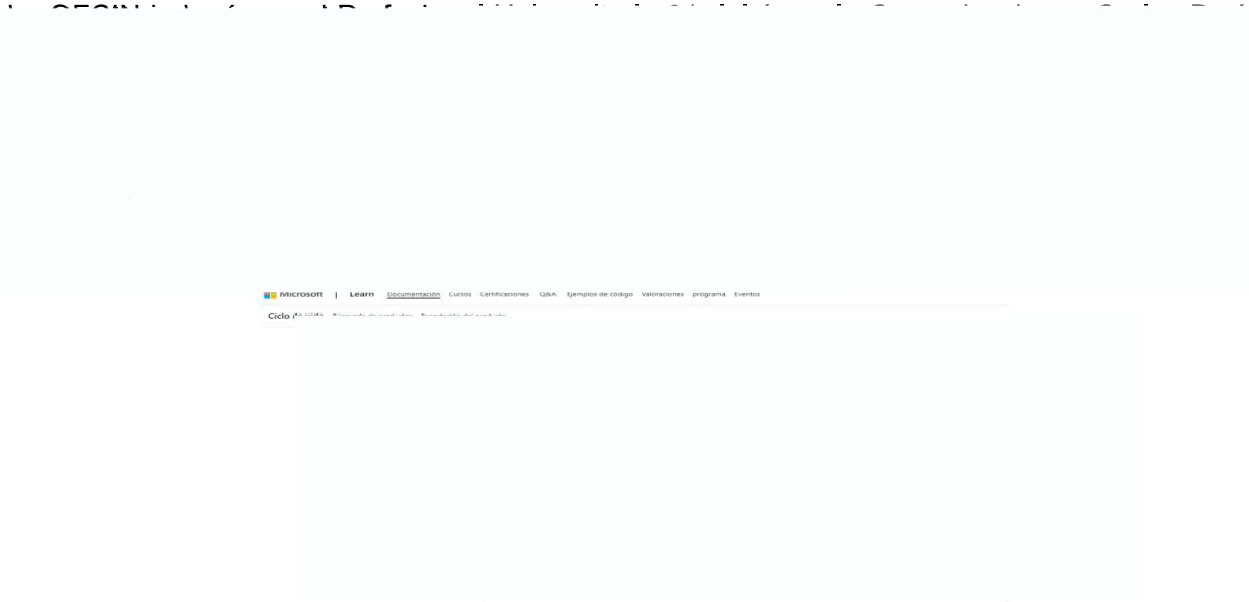


Figura 69 Pantalla vigencia SharePoint 2013

Fuente: https://support.microsoft.com/es-es/office/fin-del-soporte-t%C3%A9cnico-para-office-2013-90e4b0d1-098f-4656-b6e7-8b13b67ed62f – Consultado 19-04-2023

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 realizar de manera prioritaria la migración a la versión más reciente de la herramienta SharePoint en lo referente al sitio Web de la Entidad, obteniendo así todas las ventajas en términos de seguridad, funcionalidad, escalabilidad y gestión de costos, además de ser prioritario contar con un proveedor o un profesional al interior de la Caja Honor que ejecute las funciones de Web Master, que se encargue 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.

Adicionalmente, se validó el tema relacionado con Accesibilidad Web, revisando el cumplimiento de los lineamientos impartidos mediante la Norma Técnica Colombiana NTC 5854 de 2011, para lo cual con el apoyo de la OAGRI se efectúo escaneo al Sitio Web mediante las herramientas AChecker Web Accessibility Checker y Total Validator, cuyo resultado se presenta en el siguiente archivo.

AChecker Web
Accessibility Checker

Oportunidad de Mejora Preventiva 3.

La OFCIN recomienda a la SUVIP - ARCOM en coordinación con la OAINF y la OAGRI realizará de manera prioritaria las gestiones necesarias para la migración a la versión más reciente de la herramienta SharePoint en lo referente al Sitio Web, obteniendo así todas las ventajas en términos de seguridad, funcionalidad, escalabilidad y gestión de costos y la designación de un proveedor o un profesional al interior de la Entidad con funciones taxativas para ejercer como Web Master, quien será el encargado de programar y mantener el sitio web para que funcione correctamente, aplicando actualizaciones de los requisitos normativos y verificación de los 4 principios fundamentales de la Norma Técnica – NTC 5854 de 2011 de accesibilidad Web, tendiente a ofrecer un sitio web fácil de usar y que brinde una experiencia segura y agradable a los usuarios; de tal forma que se minimicen riesgos asociados con RSI031 - Pérdida de Información, RSI029 - Pérdida de la Integridad del Activo de Información, RSI036 – Pérdida de Confidencialidad del Activo de Información; R010 - Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad; así como el incumplimiento a las Dimensiones de MIPG V5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.

Igualmente, acorde con el autodiagnóstico realizado en la Matriz ITA de 29/09/2022, en el cual se observó que el Nivel de Cumplimiento fue de 100 sobre 100 puntos y una vez obtenido el Consolidado de Resultados del Reporte de Auditoría ITA 0998 para el Periodo 2022 Número de documento NI 860021967 realizado por la PGN con un Puntaje de 86 sobre 100 puntos, la OAPLA mediante email del 17 de enero de 2023 requirió a la Procuraduría aclaración al respecto sin que a la fecha se haya recibido respuesta, por lo que la OFCIN recomienda que se reitere a dicha Entidad la importancia de que se nos aclare el tema, de forma tal, que se logre identificar los ajustes que se deben aplicar con el fin de iniciar un plan de acción y así avanzar en la mejora continua el proceso, para que en próximas mediciones se alcance el máximo nivel de cumplimiento por cada uno de los ítems que componen dicha matriz en lo pertinente a Accesibilidad Web, acorde a la NTC 5854:2011.

Recomendación 4.

La OFCIN recomienda a la OAPLA, reiterar a la PGN la importancia del suministro de aclaraciones frente al puntaje asignado a Caja Honor teniendo en cuenta el autodiagnóstico realizado en la Matriz ITA de 29/09/2022, en el cual se observó que el Nivel de Cumplimiento fue

de 100 sobre 100 puntos y una vez obtenido el Consolidado de Resultados del Reporte de Auditoría ITA 0998 para el Periodo 2022 Número de documento NI 860021967 realizado por la PGN con un Puntaje de 86 sobre 100 puntos; de forma tal, que se logre identificar los ajustes que se deben aplicar con el fin de iniciar un plan de acción y así avanzar en la mejora continua el proceso para que en próximas mediciones se alcance el máximo nivel de cumplimiento por cada uno de los ítems que componen dicha matriz en lo pertinente a Accesibilidad Web, acorde a la NTC 5854:2011.

7. Conclusiones y/o Recomendaciones.

Conclusiones.

1.1. Una vez finalizada la revisión de la documentación suministrada por OAGRI y OAINF, referente a la gestión realizada frente a los procesos de Seguridad de la Información y Ciberseguridad, se puede concluir que desde los procesos de Riesgos e Informática se cuenta con personal idóneo para gestionar los procesos antes citados, tendientes a garantizar la seguridad de la información de la Entidad, preservando los pilares fundamentales de la misma como son Integridad, Confidencialidad y Disponibilidad. Evidenciando, además, que se cuenta con herramientas de monitoreo permanente 7x24 los 365 días del año sobre la plataforma tecnológica utilizada por Caja Honor para su operación.

1.2. OAGRI cuenta con el equipo de profesionales para dar atención a lo relacionado con los Sistemas de Información, Seguridad y Ciberseguridad, asimismo se identificó que se está gestionado adecuadamente el monitoreo sobre los indicadores en gestión de seguridad y monitoreo de sitios web.

Lo anterior, dando cumplimiento a lo definido en las 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 y 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.

1.3. Respecto a la Accesibilidad Web, teniendo en cuenta el autodiagnóstico realizado en la Matriz ITA, es importante que una vez se obtenga la respuesta por parte de la Procuraduría General de la Nación, se realiza la confrontación de la información, tendiente a identificar los ajustes a que haya lugar con el fin de iniciar un plan de acción y en próximas mediciones alcanzar el máximo nivel de cumplimiento por cada uno de los ítems que componen dicha matriz.

Como resultado del ejercicio auditor y en cumplimiento a las Directrices dadas por el DAFP relacionadas con MIPG, la OFCIN generó 3 Oportunidad de Mejora y 4 Recomendaciones tendientes a la mejora continua de los procesos.

Tabla 16 Oportunidades de Mejora y Recomendaciones – Auditoría SARSICI – NTC 5854:2011

#	OPORTUNIDADES DE MEJORA
1	**OMC 1**: En la prueba de recorrido con el consultor de seguridad de OAGRI, se evidenció que para obtener la información de Eventos / Incidentes correspondiente al primer trimestre de la vigencia 2023, fue necesario hacerlo manualmente, seleccionando todos los datos de la Consola del Centro de Servicios y con la opción copiar llevarlos a un archivo Excel, observando además que no se cuenta con la información relacionada con la respuesta o solución del incidente o evento, la cual se debió complementar igualmente de forma manual; por lo tanto, la OFCIN recomienda a la OAGRI, estudiar la posibilidad con el proveedor de la herramienta Centro de Servicios, la creación e implementación de una opción de reportes automáticos de Eventos / Incidentes registrados en un periodo dado, tendiente a optimizar el proceso y a preservar los pilares fundamentales de seguridad de la información indicados por el Estándar ISO:27001:2013 como son la Integridad, Confidencialidad y Disponibilidad, dando cumplimiento a lo establecido en el ítem A12 del Anexo A del citado Estándar y a las buenas prácticas aplicables al manejo de la información; GR-NA-MA-009 Manual Seguridad de la Información y Ciberseguridad, versión 3, aprobado el 25-06-2021, de tal forma que se minimice la materialización de posibles riesgos asociados RSI030 – Información Errada, RSI036 – Pérdida de Confidencialidad del Activo de Información, así como el cumplimiento a las Dimensiones de MIPG Versión 5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.
2	**OMC 2**: La OFCIN recomienda a la OAINF implementar y mantener un control estricto respecto a la gestión de usuarios de los servicios tecnológicos alineado con las políticas de seguridad de la información establecidas al interior de la Entidad, puesto que situaciones relacionadas con usuarios que nunca se han logueado, que su último inicio de sesión ha superado los cinco días calendario, usuarios que ya no prestan sus servicios en la Entidad y continúan con el usuario Activo, entre otros, tal como se refiere en el numeral 5.3.9. del presente informe; no corresponden a una buena práctica de seguridad de la información, ni a lo descrito en la Guía de Operación Crear, Modificar e Inactivar Usuarios y Nombres de Recursos de TI, Código IT-NA-GU-009, V15 de Fecha 8/Feb/2023, ni da cumplimiento a lo requerido por el Estándar ISO 27001:2013, Numeral A9 del Anexo A “Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios”, ni preserva los pilares fundamentales de Seguridad de la Información como son integridad, confidencialidad y disponibilidad de la misma, conllevando a la posible materialización de riesgos relacionados con RSI031 - Pérdida de Información, RSI030 – Información Errada, R010 - Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad; así como el incumplimiento a las Dimensiones de MIPG V5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.

	Por otra parte, la OFCIN recomienda a la OAINF (Mesa de Ayuda) buscar los mecanismos que permitan registrar en el AD los datos principales de los colaboradores de la Entidad, tales como identificación correcta, nombres y apellidos y proceso o área al que corresponden; de tal forma que al generar el reporte se cargue dicha información principal y no se tengan que realizar procesos manuales como complementar en Excel el número de identificación de los usuarios.
3	**OMP3:** La OFCIN recomienda a la SUVIP - ARCOM en coordinación con la OAINF y la OAGRI realizará de manera prioritaria las gestiones necesarias para la migración a la versión más reciente de la herramienta SharePoint en lo referente al Sitio Web, obteniendo así todas las ventajas en términos de seguridad, funcionalidad, escalabilidad y gestión de costos y la designación de un proveedor o un profesional al interior de la Entidad con funciones taxativas para ejercer como Web Master, quien será el encargado de programar y mantener el sitio web para que funcione correctamente, aplicando actualizaciones de los requisitos normativos y verificación de los 4 principios fundamentales de la Norma Técnica – NTC 5854 de 2011 de accesibilidad Web, tendiente a ofrecer un sitio web fácil de usar y que brinde una experiencia segura y agradable a los usuarios; de tal forma que se minimicen riesgos asociados con RSI031 - Pérdida de Información, RSI029 - Pérdida de la Integridad del Activo de Información, RSI036 – Pérdida de Confidencialidad del Activo de Información; R010 - Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad; así como el incumplimiento a las Dimensiones de MIPG V5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación. Igualmente, acorde con el autodiagnóstico realizado en la Matriz ITA de 29/09/2022, en el cual se observó que el Nivel de Cumplimiento fue de 100 sobre 100 puntos y una vez obtenido el Consolidado de Resultados del Reporte de Auditoría ITA 0998 para el Periodo 2022 Número de documento NI 860021967 realizado por la PGN con un Puntaje de 86 sobre 100 puntos, la OAPLA mediante email del 17 de enero de 2023 requirió a la Procuraduría aclaración al respecto sin que a la fecha se haya recibido respuesta, por lo que la OFCIN recomienda que se reitere a dicha Entidad la importancia de que se nos aclare el tema, de forma tal, que se logre identificar los ajustes que se deben aplicar con el fin de iniciar un plan de acción y así avanzar en la mejora continua el proceso, para que en próximas mediciones se alcance el máximo nivel de cumplimiento por cada uno de los ítems que componen dicha matriz y para el caso que nos ocupa en el numeral 6 del presente informe, lo pertinente a Accesibilidad Web, acorde a la NTC 5854:2011.

Fuente: Elaboración propia OFCIN, abril de 2023.

#	RECOMENDACIONES
1	**Recomendación 1**: Dado lo anteriormente expuesto, la OFCIN recomienda a la OAINF en conjunto con OAGRI llevar a cabo la aplicación de las acciones pertinentes para remediar las vulnerabilidades relacionadas en la Tabla 5 Vulnerabilidades_ IP 172.20.0.6 Nivel Alto_Escaneo herramienta Ossim Alien Vault y suministrar las evidencias de las acciones aplicadas, a fin 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, atendiendo las buenas prácticas de seguridad de la información y los lineamientos impartidos por la ISO 27001:2013, minimizando la materialización de posibles riesgos asociados con RSI031 - Pérdida de Información, R010 - Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad; así como el incumplimiento a las Dimensiones de MIPG V5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación. Asimismo, verificar la pertinencia de la actualización del procedimiento código GR-NA-PR-028, no solo en su contenido sino en la normatividad vigente aplicable y responsables del mismo. Por otra parte, verificar y suministrar evidencias de las acciones aplicadas para subsanar las vulnerabilidades de Nivel Alto y Medio encontradas en el escaneo Ossim Alien Vault, las cuales se relacionan en la tabla 6 del presente informe.
2	**Recomendación 2:** Así las cosas, la OFCIN recomienda a la OAINF en coordinación con la OAGRI, asegurarse mediante la ejecución de un nuevo test en ambiente de pruebas que se hayan subsanado todas las vulnerabilidades(si el resultado de dicho test fue exitoso, es decir, no se encontraron vulnerabilidades, se pasa el desarrollo a producción, de lo contrario continuará en ambiente de pruebas hasta que se subsanen tales vulnerabilidades); y una vez el desarrollo se encuentre en producción se realice nuevamente el escaneo de vulnerabilidades para 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 tendiente a preservar los criterios de seguridad de la información emanados de la ISO 27001:2013 y minimizar la materialización de riesgos asociados con RSI031 - Pérdida de Información, Pérdida de Confidencialidad del Activo de Información y con el fin de dar cumplimiento a las Dimensiones de MIPG V5, 3ª Gestión con Valores para Resultado y 5ª Información y Comunicación.
3	**Recomendación 3:** Teniendo en cuenta las políticas establecidas en Caja Honor para la ejecución del proceso de restauración es importante que la OAINF desarrolle dicho proceso con la periodicidad indicada, realizando las pruebas pertinentes para verificar la funcionalidad e integridad física y lógica que garanticen el correcto funcionamiento de las copias de seguridad. Lo anterior, con el propósito de proteger y ayudar a la Entidad a recuperarse en caso de presentarse algún evento no planificado como fallos en el hardware o software, o causados por un ser humano como la eliminación accidental de datos, ataques maliciosos (virus o malware), que conlleven a la posible pérdida de información. Además de suministrar la completitud de la información correspondiente al periodo evaluado, que permita a la OFCIN realizar los análisis de información pertinente en aras de emitir las recomendaciones a que haya lugar para apoyar el mejoramiento continuo del proceso; atendiendo las buenas prácticas de seguridad de la información, Guía de Operación Generación de Backups y Proceso de Restauración, Código IT-NA-GU-007, V13 del 08-Feb-2023, además de lo descrito

	en el nu e minimizar la mat Calidad y Entreg nformación, RSI03(egales y/o Norma nsiones de MIPG nicación.
4	La OF(ministro de aclarac cuenta el autodia servó que el Nive btenido el Consol iodo 2022 Númer taje de 86 sobre se deben aplicar ontinua el proces nivel de cumpli ra el caso que nc cesibilidad Web, a

Fuente: Elabora

En los anteric stablecido en el cronograma de auditoría 2023, encaminada a la mejora continua de los procesos.

Cordialmente.

Firmado por:
MARTHA CECILIA MORA CORREA
2023/05/04 03:03:12
CC
55165780

MARTHA CECILIA MORA CORREA
Jefe Oficina de Control Interno

Elaboró:

Flor Alba Roncancio Gachancipa.
Auditor Oficina de Control Interno.