FECHA DE EMISIÓN DEL INFORME	Día:	31	Mes:	10	Año:	2024

Informe No.	**ASIG No. 24** – Informe Final
Nombre del Seguimiento	Verificación, Seguimiento a la Implementación de Modelo de Seguridad y Privacidad de la Información - MSPI. Ministerio de las TIC. + Resolución 0500 de 2021. FURAG - Política de Protección de Datos Personales - Política General de Seguridad y Privacidad de la Información - Política de Relación con Proveedores - Política servicio de correo electrónico corporativo.
Objetivo del Seguimiento	Verificar y dar seguimiento a la Implementación de Modelo de Seguridad y Privacidad de la Información - MSPI. Ministerio de las TIC. + Resolución 0500 de 2021. FURAG - Política de Protección de Datos Personales - Política General de Seguridad y Privacidad de la Información - Política de Relación con Proveedores - Política servicio de correo electrónico corporativo, en la ADRES
Alcance del Seguimiento	Verificar y dar seguimiento a la Implementación de la Política de Protección de Datos Personales - Política General de Seguridad y Privacidad de la Información - Política de Relación con Proveedores - Política servicio de correo electrónico corporativo y alcance a los procedimientos.
Normatividad	• Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", señalando en su artículo 2.2.21.5.3, modificado por el artículo 17 del Decreto 648 de 2017, que "las Unidades u Oficinas de Control Interno o quien haga de sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control". • Resolución Número 00500 de Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" • Decreto 767 de 2022: "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". • Ley de Transparencia 1712 de 2014: La cual tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información. • Resolución Nro. 001519 de 24 de agosto de 2020: 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. • Decreto 612 de 2018 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado. • Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Ley 1712 de 2014. "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones." • Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022. • MRAE. D.M Documento Maestro - Marco de Referencia de Arquitectura Empresarial. • Gobierno Digital - Documento Maestro del Modelo de Seguridad y Privacidad de la Información – Octubre 2021 • Anexo 3: Condiciones mínimas técnicas y de seguridad digital (cumplimiento de la Ley 1712 de 2014 y la Resolución 1519 de 2020 - MinTIC). • Política de Protección de Datos Personales V2 – 29 de diciembre 2022 • Política General de Seguridad y Privacidad de la Información V4 – 29 de diciembre 2022 • Política Relación con Proveedores V1 – Noviembre 2023 • Política de Uso del Servicio de Correo Electrónico Corporativo V1 – Noviembre 2023 • Procedimiento Gestión de la Seguridad de la Información V3 – OSTI-PR09 • Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas Versión 6. • Manual de Políticas Específicas de Seguridad y Privacidad de la Información. • MRAE. D.M Documento Maestro - Marco de Referencia de Arquitectura Empresarial. • Manual de Políticas Específicas de Seguridad y Privacidad de la Información • Instructivo de la Política para el Tratamiento de Datos Personales- Función Pública

1. ANÁLISIS Y OBSERVACIONES

La Oficina de Control Interno (OCI), en su Rol de "Evaluación y Seguimiento", incluyó en el Plan Anual de Auditorías Internas de la presente vigencia 2024, la Verificación, Seguimiento a la Implementación de Modelo de Seguridad y Privacidad de la Información - MSPI. Ministerio de las TIC. + Resolución 0500 de 2021. FURAG - Política de Protección de Datos Personales - Política General de Seguridad y Privacidad de la Información - Política de Relación con Proveedores - Política servicio de correo electrónico corporativo. A continuación se da inicio a la presente auditoria:

PLANEACIÓN DE LA EVALUACIÓN:

- **Comunicación de la evaluación**:
  - Mediante Oficio Remisorio Radicado No.: 20241100554753 del 7 de octubre de 2024, se informa según el plan de anual de auditorías el inicio de la evaluación a la Gobierno Digital - Documento Maestro del Modelo de Seguridad y Privacidad de la Información – Octubre 2021 a la Dirección de Gestión de Tecnologías de Información Y Comunicaciones y Oficina Asesora de Planeación y Control de Riesgos, sobre el mecanismo de la evaluación y solicitudes de información en su alcance.
- **Acampamiento INSITU:**
  - A partir del periodo establecido para esta evaluación según el plan anual de auditoras de la presente vigencia será comprendido entre el 1 al 31 de octubre de 2024, visita de auditoría a la Dirección de Gestión de Tecnologías de Información y Comunicaciones y la Oficina Asesora de Planeacion y Control de Riesgos, sobre el mecanismo de la evaluación y solicitudes de información en su alcance.

METODOLOGÍA

Para realizar la verificación de la presenta auditoría con el objeto de obtener evidencia suficiente, confiable y verídica que le permita a la Oficina de Control Interno (OCI) fundamentar sus opiniones, conclusiones y recomendaciones, en el marco de Resolución Número 00500 de Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" y normatividad vigente, imparte de lineamientos en pro y mejora en materia de implementación y adopción de buenas prácticas, con el objeto de verificar el cumplimiento en gestión del Modelo de Seguridad y Privacidad de la Información (MSPI) en la ADRES.

Dado lo anterior, se utilizó la técnica de "Observación", que consiste en evaluar que los procedimientos de la Política de Protección de Datos Personales, Política General de Seguridad y Privacidad de la Información, Política de Relación con Proveedores y la Política servicio de correo electrónico corporativo, cumplan con la normatividad Vigente.

Se solicita adicionalmente para la evaluación la siguiente información:

- Contrato ADRES-CTO-868-2023 Objeto: Prestar el Servicio de Centro de Operaciones de Seguridad para la ADRES (SOC). Verificación de la herramienta SOC – INSITU.
- Resolución en construcción OAPCR – Arquitectura Empresarial (AE) "Por medio de la cual se crea el Subcomité de Arquitectura Empresarial de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud ADRES, se establecen sus funciones y se definen los roles relacionados con la adopción del Marco de Referencia de Arquitectura Empresarial (MRAE), como habilitador transversal de la Política de Gobierno Digital".
- Matriz de Riesgos de Seguridad de la Información
- Reporte de Activos de Seguridad de la Información.
- Nivel de Madurez de la Seguridad de la Información.
- Entre otros documentos que se requieran en el marco de la normatividad vigente que de alcance a la auditoria.

Se revisa el Manual para la Gestión de Riesgos DIES-MA01 y Guía para la Administración del Riesgo y

el diseño de controles en Entidades públicas Versión 6. en su rol de enfoque en el subsistema de administración de riesgos de la ADRES - Sistemas Integral de Gestión de Riesgos (SIGR) - Seguridad de la información y Protección de Datos Personales que (contempla los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, el cual se tuvo en cuenta en el cumplimiento de controles al Procedimiento Gestión de la Seguridad de la Información V3 – OSTI-PR09 y Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03 establecidos e implementados y cargue de los mismos en la formulación en EUREKA.

Por último se realiza la verificación al Servicio de Centro de Operaciones de Seguridad para la ADRES (SOC).

De acuerdo con lo anterior, para generar el informe preliminar, se organizó mesas de trabajo por la auditora TIC-OCI, sobre el estado actual de la implementación del MSPI en la Entidad así:

Tabla 1. Mesa de Trabajo OAPCR – ANEXOS

EQUIPO DE TRABAJO – ANEXOS 1				
ANEXOS	**NOMBRE COMPLETO**	**CORREO**	**DEPENDENCIA**	**FECHA Y HORA MESA DE TRABAJO**
Matriz de Riesgos de Seguridad de la Información Reporte de Activos de Seguridad de la Información. Nivel de Madurez de la Seguridad de la Información.	Rodolfo Oswaldo Uribe Duarte	magaly.tello@adres.gov.co	Oficina Asesora de Planeacion y Control de Riesgos	**22 de octubre 2024** **10:00 AM A 12:00 PM**
Mapa de Riesgos de Seguridad de la Información	Diana Esperanza Torres Rodríguez	dianae.torres@adres.gov.co		**28 de octubre 2:10 PM**

Tabla 2. Mesa de Trabajo DGTIC – ANEXOS

EQUIPO DE TRABAJO – ANEXOS 2				
ANEXOS	**NOMBRE COMPLETO**	**CORREO**	**DEPENDENCIA**	**FECHA Y HORA MESA DE TRABAJO**
Contrato UT SOC CTO-868-2023 Validación En Plataforma SOC	Magaly Tello Ramirez	magaly.tello@adres.gov.co	Dirección de Gestión de Tecnologías de Información y Comunicaciones	**11 de octubre 2024** **11:00 AM A 12:00 PM**
	Guillermo Manuel Benitez Rodriguez	guillermo.benitez@adres.gov.co		

RESULTADOS DE LA VERIFICACIÓN Y SEGUIMIENTO

Con el fin de garantizar y dar cumplimiento al objeto y alcance del presente informe preliminar, se presenta el resultado de la verificación y seguimiento por la Oficina de Control Interno (OCI), en el marco de la Resolución Número 00500 de Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" implementado en la Entidad de la siguiente forma:

- **ARTÍCULO 5.** La estrategia de seguridad digital. Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

  El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

  La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital. Adicionalmente, la estrategia de seguridad digital debe:

  1. Ser aprobada a través de un acto administrativo de carácter general.
  2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.
  3. Establecer los roles y responsabilidades al interior de la Entidad asociados a la seguridad digital.
  4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la Entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces.
  5. La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.
  6. Aplicar las demás consideraciones que a juicio de la Entidad contribuyan a elevar sus estándares de seguridad digital.

De acuerdo con lo anterior y dando alcance al presente informe, se verifica el cumplimiento de implementación MSPI en la Entidad en cuanto a la:

- Política de Protección de Datos Personales V2 – 29 de diciembre 2022

- Política General de Seguridad y Privacidad de la Información V4 – 29 de diciembre 2022
- Política Relación con Proveedores V1 – Noviembre 2023
- Política de Uso del Servicio de Correo Electrónico Corporativo V1 – Noviembre 2023

- **POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES**

La ADRES en su condición de responsable declara proteger el derecho a la privacidad y el buen nombre de los titulares durante el tratamiento de los datos personales, por tal razón se rige por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

El objeto de la política de Protección de Datos Personales en la ADRES, es establecer los criterios para la recolección, almacenamiento, uso, circulación y supresión de los datos personales, en la operación de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES, para la debida implementación, verificación y mejora continua del cumplimiento del régimen de protección de datos personales.

De acuerdo con lo expuesto se presenta los siguientes documentos que se encuentran en EUREKA y que dan alcance a la política:

Tabla 3. Documentación – DATOS – EUREKA

Nombre	Código	Tipo	Versión	Fecha versión	Estado
Gestión de Copias de Respaldo de Bases de Datos	OSTI-PR20	Procedimiento	1	30/12/2021 11:00	Activo
Esquema de Metadatos para la Gestión de Documentos Electrónicos	GDOC-PT02	Protocolo	2	15/01/2024 23:59	Activo
Bases de Datos Reparto Conciliaciones	GJUR-FR01	Formato	1	4/12/2019 0:00	Activo
Bases de Datos Reclamaciones	GJUR-FR02	Formato	1	4/12/2019 0:00	Activo
Gestión de Datos Abiertos	OSTI-PR10	Procedimiento	2	18/03/2020 0:00	Activo
Autorización para el Tratamiento y Uso de Datos Personales	GETH-FR38	Formato	3	13/06/2023 17:00	Activo
IPS Base de Datos Régimen Subsidiado	GEPR-FR05	Formato	1	23/04/2019 0:00	Activo
Base de Datos de Validación Traslados VS Movimientos Bancarios	GEPR-FR10	Formato	1	23/04/2019 0:00	Activo
Auditoría Base de Datos	VALR-PR38	Procedimiento	3	27/01/2021 0:00	Activo
Solicitud Actualización Datos RNEC	VALR-PR47	Procedimiento	1	27/01/2021 0:00	Activo
Protección de Datos Personales	APTI-PL02	Política	2	29/12/2022 23:59	Activo
Solicitud de Consulta WEB de Base de Datos Única de Afiliados BDUA	OSTI-FR09	Formato	2	27/04/2022 23:59	Activo
Autorización al Servicio de Consulta WEB de la Base de Datos Única de Afiliados BDUA	OSTI-PR17	Procedimiento	2	27/04/2022 23:59	Activo
Base de datos de Control de Reintegros por Servicios y Tecnologías No Financiados por UPC	VERS-FR02	Formato	1	5/11/2021 12:02	Activo
Base de Datos Control Reintegros Reclamaciones	VERS-FR07	Formato	1	5/11/2021 12:01	Activo

Según lo anterior frente a la Política de Protección de Datos Personales V2 – 29 de diciembre 2022, si es importante que la Oficina Asesora de Planeación y Control de Riesgos (OAPCR) solicite el Oficial de Datos Personales de la vigilancia y control de la aplicación que tendrá la labor de estructurar, diseñar y administrar el plan o programa que permita a la Entidad cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente. (Revisar la Política rol y funciones en la Política de Protección de Datos Personales V2 – 29 de diciembre 2022)

Observación 1:

De acuerdo con la **Tabla 2**, se puede verificar que la Entidad no cuenta con un procedimiento y un manual que integre y abarque todas las actividades y procesos relacionados con la recopilación, uso, almacenamiento, transferencia y disposición de datos personales dentro de la ADRES. Esto incluye, pero no se limita a datos de servidores públicos, contratistas, proveedores, ciudadanía en general y cualquier otro tercero cuya información personal sea objeto de tratamiento o haga parte del desarrollo y cumplimiento de sus funciones misionales. Todos los servidores públicos en virtud de su relación con la Entidad, tengan acceso a datos personales o participen en su tratamiento, sujetos a la Política de Protección de Datos Personales V2 – 29 de diciembre 2022 de la Entidad. Con relación de lo expuesto se da alcance al proceso para definir la necesidad de un Oficial de Datos Personales de la vigilancia y control de la aplicación de la presente Política de Protección de Datos Personales.

Lo anterior hace referencia a la Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Ley 1712 de 2014. "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.", Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022. por lo cual se debe tener en cuenta en la construcción de procedimiento y manual lo siguiente:

Artículo 13. Políticas de Tratamiento de la información. Los responsables deberán desarrollar sus políticas para el tratamiento de los datos personales y velar por el cumplimiento a las mismas.

Las políticas de Tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:

1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.
2. Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.
3. Derechos que le asisten como Titular.
4. Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
5. Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
6. Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

Cualquier cambio sustancial en las políticas de tratamiento, en los términos descritos en el **artículo 5°** del presente decreto, deberá ser comunicado oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas.

Condición:

De la revisión efectuada por parte de la OCI, se observó que no se cuenta con un procedimiento y un manual que integre y abarque todas las actividades y procesos relacionados con la recopilación, uso, almacenamiento, transferencia y disposición de datos personales dentro de la ADRES, que de alcance a la Política de Protección de Datos Personales V2 – 29 de diciembre 2022 de la Entidad, de acuerdo con los criterios establecidos en el Decreto Nacional 1377 de 2013 - Artículo 13. Políticas de Tratamiento de la información y a la falta de un Oficial de Datos Personales de la vigilancia y control de la aplicación de la presente Política de Protección de Datos Personales.

Criterio:

Lo anterior da incumplimiento a la Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Ley 1712 de 2014. "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones." -l Decreto Nacional 1377 de 2013 - Artículo 13. Políticas de Tratamiento de la información, respecto a que no se cuenta con un procedimiento y un manual que integre y abarque todas las actividades y procesos relacionados con la recopilación, uso, almacenamiento, transferencia y disposición de datos personales dentro de la ADRES. Esto incluye, pero no se limita a datos de servidores públicos, contratistas, proveedores, ciudadanía en general y cualquier otro tercero cuya información personal sea objeto de tratamiento o haga parte del desarrollo y cumplimiento de sus funciones misionales. Todos los servidores públicos en virtud de su relación con la Entidad, tengan acceso a datos personales o participen en su tratamiento, sujetos a la Política de Protección de Datos Personales V2 – 29 de diciembre 2022 de la Entidad.

Causa:

La Política de Protección de Datos Personales V2 – 29 de diciembre 2022 de la Entidad, no cuenta un manual y un procedimiento de acuerdo con el instructivo de la Política para el Tratamiento de Datos Personales de la Función Pública según lo siguiente:

- Instructivo de la Política para el Tratamiento de Datos Personales https://www.funcionpublica.gov.co/documents/418537/1512450/Instuctivo+de+la+Pol%C3%ADtica+para+el+Tratamiento+de+Datos+Personales.pdf/f7d7cbe2-6739-46de-9f76-ee147cf1aa60?download=true
    - Deberes del Departamento Administrativo de la Función Pública como Responsable del Tratamiento de los Datos Personales:
        - ✓ k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y para la atención de consultas y reclamos.

Consecuencia:

En consecuencia, y de acuerdo con lo establecido en la Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Ley 1712 de 2014. "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones." -l Decreto Nacional 1377 de 2013 - Artículo 13. Políticas de Tratamiento de la información, se solicita a la OAPCR el incumplimiento de la formulación de acciones de

fortalecimiento para la Política de Protección de Datos Personales V2 – 29 de diciembre 2022 conlleva implicaciones, estas incluyen un aumento significativo en la vulnerabilidad de la organización a actividades de corrupción e incumplimiento de los mandatos regulatorios. Así mismo, este incumplimiento podría generar posibles sanciones legales y afectar la reputación de la Entidad.

VERIFICACION MAPA DE RIESGOS Y CONTROLES

De acuerdo con la Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas Versión 6., se informa que dado el resultado de la **observación 1** no se puede realizar la verificación de controles de riesgo hasta que no se de alcance a un procedimiento con respecto al tratamiento de datos personales.

RESPUESTA POR LOS AUDITADOS

Radicado No.: 20241300570163 Fecha: 2024-11-22 17:03

Sobre este tema queremos comentar desde la OAPCR que la política de protección de datos personales, actualmente definida, se encuentra bajo la responsabilidad de la Directora Administrativa y Financiera como se evidencia en la definición de la política; no obstante, dado el direccionamiento emitido por el Señor Director, en la OAPCR estamos gestionando esta política, para lo cual se encuentra en proceso la vinculación de un funcionario para fortalecer el equipo de trabajo de riesgos con el fin de atender la gestión de la protección de datos personales.

En tal sentido la OAPCR se encuentra definiendo:

- *Instructivo para el registro de bases de datos ante la SIC.*
- *Actualización del instrumento de registro de bases de datos.*
- *Plan de gestión de datos personal.*
- *Contenido temático para capacitación en protección de datos personales.*

Lo anterior como parte integral del Manual de Protección de Datos Personales y teniendo en cuenta además, el Rediseño Institucional que se está adelantando en la ADRES, así como la redefinición del Mapa de Valor de Procesos de la ADRES, que establecerán si las actividades asociadas a esta política harán parte de los procedimientos de gestión y operación de los procesos en la primera línea de defensa, o sí se requiera definir un procedimiento específico para este caso.

SOPORTES POR LA OCI

En concordancia con la respuesta de los auditados, se analizó nuevamente y se revisaron las siguientes resoluciones para dar alcance a las observaciones:

- ✓ Resolución Número 3486 de 2018 *"Por medio del cual se adopta la Política de Protección de Datos Personales dentro de la Administradora de los Recursos del Sistema General de Seguridad Social en Salud – ADRES" Artículo Tercero. Oficial de Protección de Datos. En consideración a la naturaleza de la ADRES, las tareas y responsabilidades del Oficial de Protección de Datos estarán a cargo de un equipo conformado por cuatro (4) servidores públicos de la Entidad, así: un (1) funcionario de la Dirección de Gestión de Tecnologías de la Información y Comunicaciones, un (1) funcionario de la Oficina Asesora Jurídica y dos (2) funcionarios de la Dirección Administrativa y Financiera.*

- ✓ Resolución Número 0000797 de 2022. *Por medio de la cual se modifica el artículo 3 de la Resolución 3486 de 2018, se designa el Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales de ADRES y se dictan otras disposiciones. Artículo 2°. Designación y ejecución de actividades del* ***Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales. La Oficina Asesora de Planeación y Control de Riesgos estará a cargo del cumplimiento de la Política de Tratamiento de Datos Personales de ADRES,*** *a través de un servidor público, en calidad de asesor asignado a esta dependencia, para el cumplimiento del rol de Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales.*

- ✓ Resolución 798 de 2022 *"Por medio de la cual se designa el Oficial de Seguridad y Privacidad de la Información de ADRES".*

  Artículo 1°. Objeto. Designar el Oficial de Seguridad y Privacidad de la Información en ADRES, así como establecer las actividades a su cargo y las responsabilidades de las dependencias frente a la implementación y sostenibilidad de la gestión de la protección de seguridad.

  Artículo 2°. Designación y ejecución de actividades del Oficial de Cumplimiento de la Política de Seguridad y Privacidad de la Información. ***La Oficina Asesora de Planeación y Control de Riesgos estará a cargo del seguimiento frente al cumplimiento de la Política de Seguridad y Privacidad*** *de la Información, a través de un servidor público, en calidad de asesor asignado a esta dependencia, para el cumplimiento del rol de Oficial de Seguridad y Privacidad de la Información.*

- ✓ Resolución Número 73194 de 2022, *"Por medio de la cual se actualizan, modifican, ratifican y aprueban las políticas que rigen la gestión en ADRES, y se dictan otras disposiciones" que designa mediante Decreto 620 de 2020 artículo 2.2.17.5.4 la* ***persona o área que asuma la función de protección de datos personales.***

RESPUESTA POR LA OCI

- A partir de las respuestas por parte del auditado, este manifestó la existencia de la Resolución Número 73194 de 2022, sin embargo esta resolución solo menciona que se debe establecer el encargado de protección de datos pero nada más, el cual concluye que en conformidad con la revisión que realizó la OCI a la Resolución Número 3486 de 2018, Resolución Número 0000797 de 2022 y Resolución 798 de 2022 la OAPCR debe realizar lo pertinente en la designación del oficial de datos personales quien en sus funciones dará el alcance y cumplimiento a la formulación e implementación de lineamientos según la normativa vigente, por lo anterior es necesario que se establecer un plan de mejora. **Observación 1**

- **POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

La ADRES reconoce que la información generada, almacenada y compartida en sus procesos es un activo esencial dentro de la Entidad, velando por tener los mecanismos apropiados para proteger la información de carácter sensible, clasificado o reservado.

La Entidad esta alineada con la Dirección Estratégica de la Entidad, establece la compatibilidad de la Política de Seguridad y Privacidad de la Información y define los siguientes objetivos de seguridad de la información:

1. Minimizar los riesgos asociados a los activos de información de la ADRES, con el fin de asegurar su confidencialidad, disponibilidad e integridad a través de la gestión del sistema de gestión.
2. Definir controles y lineamientos de aseguramiento, con el fin de salvaguardar la información de la entidad utilizando procedimientos, instrumentos y mecanismos automatizados.
3. Concientizar a funcionarios y colaboradores de la Adres de la importancia de la protección de los activos de información para promover su uso seguro a través de programas y campañas de seguridad de la información.
4. Mantener la confianza de los ciudadanos respecto de la información de la ADRES mediante la adecuada gestión de las buenas prácticas en seguridad de la información

De acuerdo con lo expuesto se presenta los siguientes documentos que se encuentran en EUREKA y que dan alcance a la política:

Tabla 3. Documentación - Seguridad - EUREKA

Nombre	Código	Tipo	Versión	Fecha versión	Estado
Plan de Tratamiento de Riesgos de Seguridad de la Información	DIES-PN02	Plan	2	3/10/2024 13:00	Activo
Programa de Capacitación en el Sistema de Gestión de Seguridad y Salud en el Trabajo	GETH-FR82	Formato	1	16/02/2024 11:54	Activo
Verificación Proceso Prioritario Seguridad del Paciente	VALR-FR63	Formato	1	20/02/2024 16:21	Activo
Gestión de Incidentes de Seguridad	OSTI-PR03	Procedimiento	3	18/03/2020 0:00	Activo
Gestión de la Seguridad de la Información	OSTI-PR09	Procedimiento	3	18/03/2020 0:00	Activo
Matriz de Identificación de Peligros y Valoración de Riesgos en Seguridad y Salud en el Trabajo	GETH-FR06	Formato	2	29/11/2019 0:00	Activo
Programa de Gestión Seguridad y Salud en el Trabajo	GETH-FR56	Formato	2	16/02/2024 11:55	Activo
Plan Anual de Trabajo Seguridad y Salud en el Trabajo SST	GETH-FR62	Formato	1	28/02/2020 0:00	Activo
Identificación de Peligros y Valoración de Riesgos en Seguridad y Salud en Trabajo	GETH-GU03	Guía	1	29/11/2019 0:00	Activo
Políticas Específicas de Seguridad y Privacidad de la Información	APTI-MA01	Manual	4	12/12/2022 23:59	Activo
Política General de Seguridad y Privacidad de la Información	APTI-PL01	Política	4	29/12/2022 23:59	Activo
Seguridad y Salud en el Trabajo	GETH-PL01	Política	5	1/12/2023 23:59	Activo
Reglamento de Higiene y Seguridad Industrial	GETH-PL03	Política	5	23/11/2023 16:02	Activo
Manual del Sistema de Gestión de la Seguridad y Salud en el Trabajo	GETH-MA01	Manual	1	30/12/2019 0:00	Activo

De acuerdo con la **Tabla 4**, se verifica en el Mapa de Riesgos de Seguridad de la Información los procedimientos Gestión de Incidentes de Seguridad V3 OSTI-PR03 y Gestión de la Seguridad de la

Información OSTI-PR09, por lo cual se deja la observación con respecto al OSTI-PR09 ya que este no cuenta con control de riesgos. (Elaboración Manual para la Gestión de Riesgos DIES-MA01 y Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas Versión 6.
La Política General de Seguridad y Privacidad de la Información definen los siguientes lineamientos para el cumplimiento de esta política:

- Revisión periódica.
- Gestionar los riesgos de seguridad de la información y ciberseguridad.
- Medir y evaluar el sistema de gestión de la seguridad de la información – SGSI implementado.
- Aplicar buenas prácticas en el desarrollo de la gestión de seguridad de la información y ciberseguridad.
- Realizar ejercicios de investigación y análisis de las amenazas de ciberseguridad que enfrenta a la entidad.
- Aplicar los controles necesarios a los activos de información teniendo en cuenta las buenas prácticas.
- Garantizar el cumplimiento de las normas, definiciones y lineamientos que se establezcan en esta materia.
- Definir e implementar las políticas específicas requeridas para la adecuada protección de los activos de información.

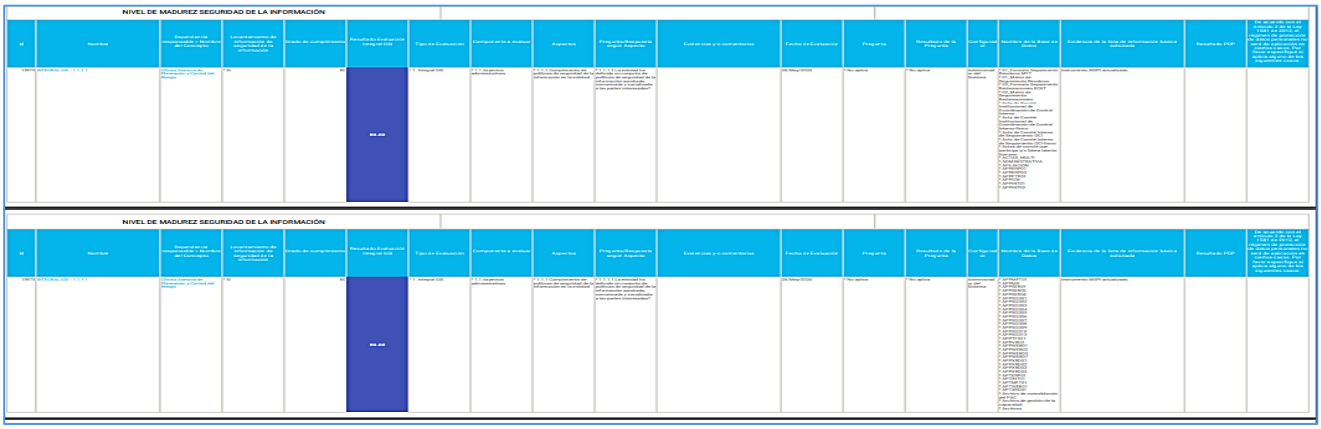
Medir y Evaluar el Sistema de Gestión de Seguridad:

La herramienta que proporciona EUREKA, para evaluar la madurez relacionada con las distintas dimensiones de la gobernanza de datos, es un instrumento de diagnóstico destinado a controlar procesos o evaluar el rendimiento de los activos de la ADRES. Su función principal es servir como punto de partida para que la OAPCR identifique mejoras posibles y actúen en consecuencia según las recomendaciones proporcionadas, que puede aplicarse con fines:

- **Descriptivos** si se utiliza como herramienta de diagnóstico para que los niveles de madurez asignados puedan ser reportados a las partes interesadas;
- **Prescriptivos** si se utilizan para identificar los niveles de madurez deseables y para proporcionar directrices sobre qué medidas de mejora implementar;
- **ambos.**

A continuación, se presenta la matriz de Madurez de Seguridad de la Información:

Ilustración 1. Matriz de Madures - Seguridad de la Información



De acuerdo con lo anterior, no se cuenta con un manual para la identificación de activos de la Entidad de acuerdo con la **Ilustración 1** y de alcance al formato Inventario de activos de información GEDO-PROC-59 según Guía para la Gestión y Clasificación de Activos de Información. y que también reporte resultados cuantitativos y cualitativos así:

- **Resultados cuantitativos:**
    - Gráfico de síntesis que describe el grado de madurez en cada dimensión.
    - Puntajes numéricos detallados en cada dimensión evaluada brindan una visión objetiva de la situación actual.

- **Resultados cualitativos:**
    - El análisis cualitativo interpreta estos puntajes, contextualiza la información, identifica logros y áreas de mejora, y aporta una comprensión más amplia y contextualizada de las particularidades del área evaluada.
    - Las recomendaciones y acciones sugeridas, basadas en los resultados detallados de la matriz, se convierten en un mapa preciso para implementar cambios y potenciar el rendimiento del área evaluada.

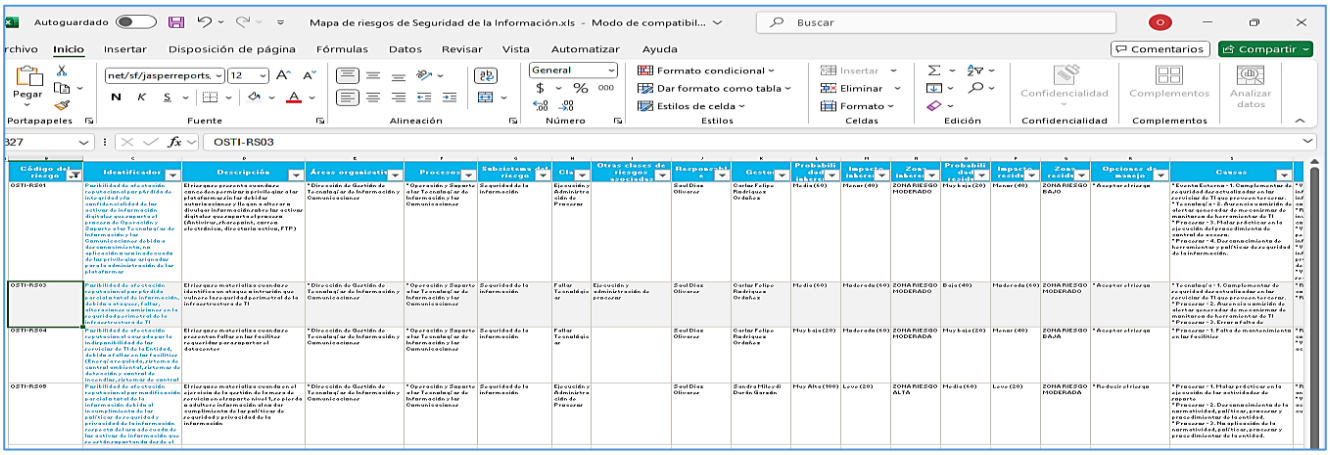
Seguridad de la Información y Ciberseguridad:

De acuerdo con lo anterior, la Entidad no cuenta con un oficial en ciberseguridad que se encargue de planear, coordinar y administrar los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la Entidad.

Matriz de Riesgos de Seguridad de la Información:

La ADRES en su modelo integrado de planeación y gestión institucional (SIGI)aplica un esquema de líneas de defensa para administrar los riesgos de gestión, corrupción y de Lavado de Activos y Financiación del Terrorismo LA/FT, seguridad de la información, crédito, liquidez entre otros. Iniciando con la identificación de riesgos siguiendo con el análisis, valoración, definición de controles, tratamiento y finaliza con el monitoreo, seguimiento y comunicación así:

Ilustración 2. Mapa de Riesgos - Seguridad de la Información - OSTI

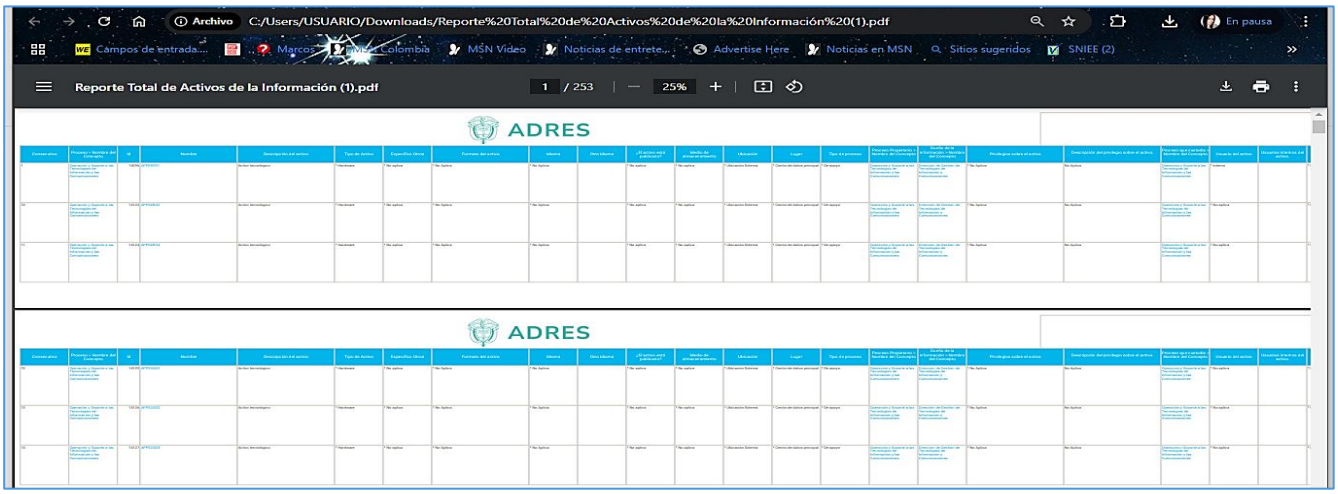


Teniendo en cuenta la **Ilustración 2** como resultado de la verificación en el mapa de riegos de seguridad de la información que reporta EUREKA, se observa que al filtrar la columna código del riesgo el procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03 cuenta con control de riesgos y con respecto al procedimiento Gestión de la Seguridad de la Información OSTI-PR09 no cuenta con control de riesgos, por lo cual se procede a dejar la observación.

Reporte de Activos de Seguridad de la Información:

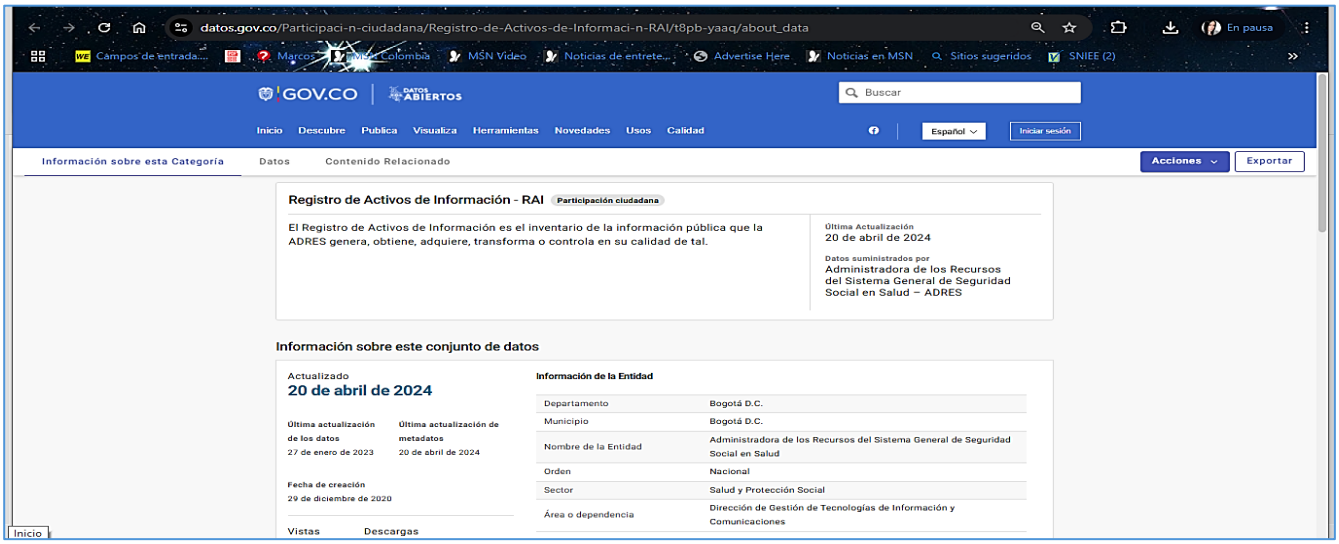
Según la **Ilustración 3** la OACPR realiza su reporte de activos con un total de 567 reportes en Seguridad de la Información teniendo en cuenta lo implementado en los procesos de la Entidad así:

Ilustración 3. Reporte Total de Activos en Seguridad de la Información



La OACPR de la ADRES reporta los Activos de Seguridad de la Información en la plataforma GOV.CO según **Ilustración 3** en el siguiente enlace: https://www.datos.gov.co/Participaci-n-ciudadana/Registro-de-Activos-de-Informaci-n-RAI/t8pb-yaaq/about_data

Ilustración 4. Reporte de Activos de Información - GOV.CO



Por otro lado, el proceso Operación y Soporte a las Tecnologías de Información y las Comunicaciones, cuenta con la Política General de Seguridad y Privacidad de la Información que da alcance al procedimiento de Gestión de Incidentes de Seguridad V3 OSTI-PR03 donde se establezca los lineamientos, las reglas e instrucciones que permitan la gestión y clasificación de los Activos de Información de la ADRES, con el fin de identificarlos, protegerlos y asegurarlos, de acuerdo con estándares de seguridad internacionales y a las prácticas y recomendaciones dadas por el Gobierno Digital.

En esta política respalda los criterios de los activos del anexo A de la norma ISO 27001:2013 con el objeto de garantizar el cumplimiento de los puntos descritos a continuación:

- Inventario de activos: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
- Propiedad de los activos: Los activos mantenidos en el inventario deben tener un propietario.
- Clasificación de la información: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- Etiquetado de la información: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la Entidad.
- Manejo de activos: Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la Entidad.
- Uso aceptable de los activos: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
- Devolución de activos: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la Entidad que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Aplicación de Controles:

Según la Política General de Seguridad y Privacidad de la Información es importante aclarar si la Entidad según los auditados no se va a Certificar en la ISO 27001:2013, proponer que alcance se le dará a los controles de la ISO/IEC 27002:2013 en cuanto a la:

- Confidencialidad: Según la norma ISO/IEC 27002:2013 es la propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Disponibilidad: Según la norma ISO/IEC 27002:2013 Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- Incidente de Seguridad: Según la norma ISO/IEC 27002:2013 es evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. Integridad: En consideración a la norma ISO/IEC 27002:2013 es la propiedad de la información relativa a su exactitud y completitud.
- Integridad: En consideración a la norma ISO/IEC 27002:2013 es la propiedad de la información relativa a su exactitud y completitud.
- Riesgo: Según la norma ISO/IEC 27002:2013, es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. Vulnerabilidad: De acuerdo con la ISO/IEC 27002:2013, es la debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Observación 2:

Se verifico en la **Tabla 4** en el Mapa de Riesgos de Seguridad de la Información el procedimiento Gestión de la Seguridad de la Información OSTI-PR09, este no cuenta con control de riesgos.

La Entidad no cuenta con un oficial en ciberseguridad que se encargue de planear, coordinar y administrar los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la Entidad.

No se cuenta con un manual para la identificación de activos de la Entidad de acuerdo con la **Ilustración 1** y de alcance al formato Inventario de activos de información GEDO-PROC-59.

Según la Política General de Seguridad y Privacidad de la Información es importante revisar si la Entidad según los auditados no se va a Certificar en la ISO 27001:2013, entonces proponer que alcance se le dará a los controles de la ISO/IEC 27002:2013.

Condición:

De la revisión efectuada por parte de la OCI, se observó que el procedimiento OSTI-PR09 no cuenta con control de riesgos, no se cuenta con un manual de activos y no se tiene controles ISO/IEC 27002:2013 según lo expuesto anteriormente en el marco de la Resolución Número 00500 de Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"

Criterio:

Lo anterior da incumplimiento a la Resolución Número 00500 de Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" que establece lineamientos que deben ser cumplidos por los responsables para la gestión y clasificación de los Activos de Información en la ADRES, sujetos a la Política General de Seguridad y Privacidad de la Información de la Entidad.

Causa:

De la revisión efectuada por parte de la OCI, se observó que el procedimiento OSTI-PR09 no cuenta con control de riesgos, no se cuenta con un manual de activos y no se tiene controles ISO/IEC 27002:2013 según la Política General de Seguridad y Privacidad de la Información

Consecuencia:

En consecuencia, y de acuerdo con lo establecido en la Resolución Número 00500 de Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", se solicita a la OAPCR y a la DGTIC que el incumplimiento de la formulación de acciones de fortalecimiento para la Política General de Seguridad y Privacidad de la Información conlleva implicaciones, estas incluyen un aumento significativo en la vulnerabilidad de la organización a actividades de corrupción e incumplimiento de los mandatos regulatorios. Así mismo, este incumplimiento podría generar posibles sanciones legales y afectar la reputación de la Entidad.

VERIFICACION MAPA DE RIESGOS Y CONTROLES

- **Verificación Mapa de Riesgos y Controles:**

En la herramienta EUREKA, se verificó la identificación de eventos de riesgo de la dependencia Dirección de Gestión de Tecnologías de la Información Y Comunicación (DGTIC), asociado al Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03, La OCI evidenció que se analizaron los aspectos metodológicos de administración de riesgos indicados en la Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas Versión 6. Riesgo de gestión **OSTI-PR03** y Riesgo de seguridad de la información: **OSTI-PR03**, partiendo de la política de administración de riesgos hasta la valoración del riesgo y seguimiento de primera línea de defensa a la efectividad de puntos de control.

Se identificó el análisis de los siguientes aspectos metodológicos de administración de los eventos de riesgo:

- Tecnología - 1. Complementos de seguridad desactualizados en los servicios de TI que proveen terceros.
- Procesos - 2. Ausencia u omisión de alertas generadas de mecanismos de monitoreo de herramientas de TI
- Procesos - 3. Error o falta de configuración en la seguridad perimetral

En la identificación de los eventos de riesgo se tuvo en cuenta los siguientes aspectos:

- Revisar y activar nuevas reglas en la configuración

- Realizar análisis de vulnerabilidades

Se verificaron los riesgos asociados al Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03, numeral 7 Desarrollo del Procedimiento, De la revisión efectuada por parte de la OCI, el riesgo de seguridad OSTI-PR03 con corte al 31octubre de 2024, correspondiente al Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03 se observó que los dos (2) puntos de control P.C., establecidos en el citado procedimiento, no están asociados al riesgo de gestión APTI-RG01. A continuación se presenta el resultado:

1. Riesgo de seguridad de la información: **OSTI-PR03**

Dado lo anterior, se observó que se dio cumplimiento a la metodología establecida por la Entidad en cuanto a identificación, análisis, valoración y seguimiento de los riesgos.

- **Riesgo de Seguridad de la Información OSTI-PR03**

La OCI verificó el nivel de aceptación de riesgo inherente y residual del evento de riesgo identificado, se observó que el riesgo residual se encuentra en nivel de aceptación (moderado) en la **POLÍTICA DE GESTIÓN DE RIESGOS – ADRES - En el numeral 7.4.3.1 DETERMINACIÓN DEL NIVEL DE RIESGO RESIDUAL, no se estableció en esta que se debe realizar cuando la zona de riesgo inherente es Moderada. Anexo 1** al presente informe – **matriz de evaluación de riesgos.**

- **Evaluación de controles:**

Para evaluar la efectividad de cada uno de los controles implementados al riesgo inherente para reducir o mitigar la probabilidad y el impacto de eventos de riesgos, la OCI evaluó frente a la evidencia aportada según los puntos de control identificados en el Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03,, numeral 7 Desarrollo del Procedimiento, cada uno de los aspectos definidos en el diseño y su adecuada ejecución. Ver documento adjunto **Anexo 1 - matriz de evaluación de controles.**

De la verificación realizada a los riesgos y controles del procedimiento de Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03, numeral 7 Desarrollo del Procedimiento de la DGTIC, se evidenció que se encuentran documentados y registrados en la herramienta EUREKA y se están aplicando los controles establecidos para los riesgos de gestión y seguridad de la información.

RESPUESTA POR LOS ADUDITADOS

Radicado No.: 20241300570163 Fecha: 2024-11-22 17:03

Respecto de estas observaciones, solicitamos realizar una mesa de trabajo entre la OCI y los responsables de gestionar los procedimientos mencionados y sus riesgos asociados, con el fin de entender estas observaciones, para aclarar las inquietudes y de esta forma la OCI pueda generar las observaciones que se deriven de este entendimiento.

RESPUESTA POR LA OCI

En conformidad con la respuesta de los auditados, se realiza la mesa de trabajo entre la OAPCR, DGTIC y la OCI el 2 de diciembre 2024 solicitada por el equipo auditor de esta reunión se llegó a las siguientes conclusiones:

- *En cuanto a los procedimientos del proceso Operación y Soporte a las Tecnologías de Información y las Comunicaciones (OSTI),* ***se recomienda*** *hacer una revisión de identificación y formulación de riesgos asociados a los puntos de control.*

- *Con respecto al tema metodológico se puede aclarar en una mesa de trabajo entre la OAPCR, DGTIC y la OCI en el cual identifiquemos si esos procedimientos de esos controles realmente están documentados o simplemente con que se anuncien en la política de riesgo es suficiente para gestionar.*

- Por otro lado, con respecto al oficial de ciberseguridad, se evidenció que la asignación de esta función de acuerdo con el Manual APTI-MA01 Políticas Específicas de Seguridad y Privacidad de la Información en el numeral 8.4 Unidad de seguridad de la información y la ciberseguridad, es competencia de la Dirección de la Adres:

  ✓ *8.4 Unidad de seguridad de la información y la ciberseguridad*

  La Junta Directiva de la ADRES, será la responsable de aprobar esta Política y la autorización de sus modificaciones.
  La Dirección de la ADRES, asigna las funciones relativas a la Seguridad de la Información y Ciberseguridad al Oficial o Responsable de Seguridad de la Información quien tendrá a cargo las funciones relativas del rol, lo cual incluye la supervisión de todos los aspectos inherentes tratados en el presente documento, el control del cumplimiento de la Política de Seguridad de la Información y Ciberseguridad, así como garantizar que las políticas específicas, procesos, procedimientos y/o controles que se deriven de esta estén alineados con la Política y ésta con las estrategias y modelos del negocio. Según lo expuesto ***la asignación de Oficial de Ciberseguridad se encuentra a cargo al Oficial o responsable de Seguridad de la Información.*** *Por lo anterior se levanta la observación.*

- *Con respecto a la ISO 27001, la entidad no está obligada a la implementación de la norma ISO/IEC 27001:2013 y a la implementación de la norma ISO/IEC 27002:2013, sin embargo, se indica en la Política de Seguridad de la Información que, si van a ejecutar una serie de controles, los cuales se están trabajando actualmente en alineación al Manual de Políticas Específicas de Seguridad y Privacidad de la Información en su alcance. Por consiguiente, sigue siendo una expectativa de implementación, no es algo que es este ya implementando y que esté formalizado en la Entidad, por lo anterior* ***se levanta la observación.***

Observación 3

- **Condición.**

De la revisión efectuada por parte de la OCI, el riesgo de seguridad OSTI-PR03 con corte al 31octubre de 2024, correspondiente al Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03 se observó que los dos (2) puntos de control P.C., establecidos en el citado procedimiento, no están asociados al riesgo de gestión APTI-RG01.

- **Criterio.**

De acuerdo con el manual de administración de riesgos DIES MA-01 versión 6 del 13 de febrero de 2024, en el numeral 14 estable: Verificar que los controles definidos para tratar los riesgos existen, funcionan y son suficientes. Así mismo, validar la operatividad y ejecución de los controles identificados en el mapa de riesgos, para el Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03, de la DGTIC, incumpliéndolo establecido por la normatividad.

- **Causa:**

Según el mapa de riesgos de gestión el Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03, no tiene establecido los controles según Manual para la Gestión de Riesgos DIES-MA01 y Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas Versión 6, esto se origina por posible falta de seguimiento y cumplimiento a los controles del citado procedimiento establecidos en el numeral 7. Desarrollo del procedimiento.

- **Consecuencia:**

El incumplimiento de la normatividad de la aplicación de los controles establecidos para el Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03, para el riesgo de gestión del proceso, puede generar posibles debilidades en las funciones de los controles aplicado a las plataformas tecnológicas de la Entidad.

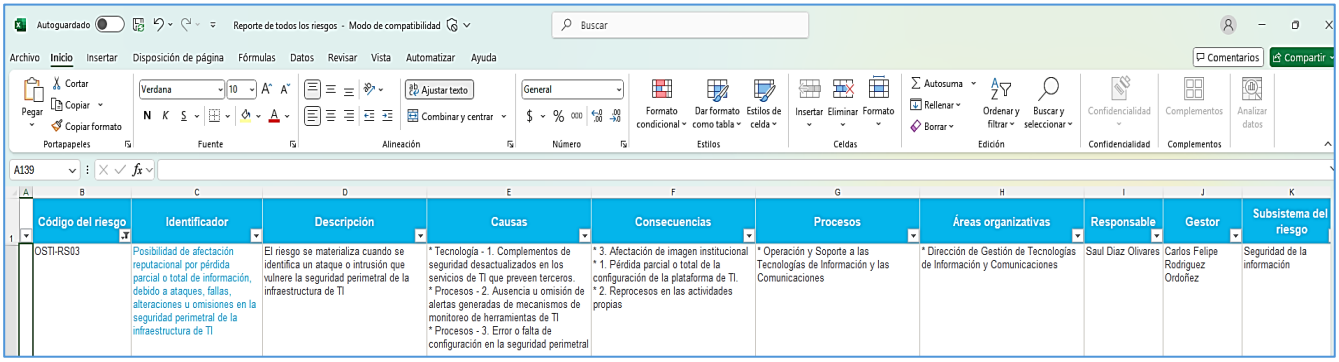
- **Controles:**

De la revisión efectuada al corte al 31 de octubre, a los controles del Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03, numeral 7 Desarrollo del Procedimiento de la DGTIC, se verificó la ejecución y aplicación de los controles por parte de la OCI, a través de la matriz de evaluación de riesgos y controles **Anexo 1- matriz de evaluación de controles**, observándose que no hay controles que apliquen en el proceso y soportes que no se encuentran almacenados en la herramienta EUREKA y los Links de acceso a los correspondientes archivos. Sin embargo, se generó la **Observación 3,** para los controles del riesgo de gestión y controles de corrupción del proceso de la DGTIC.

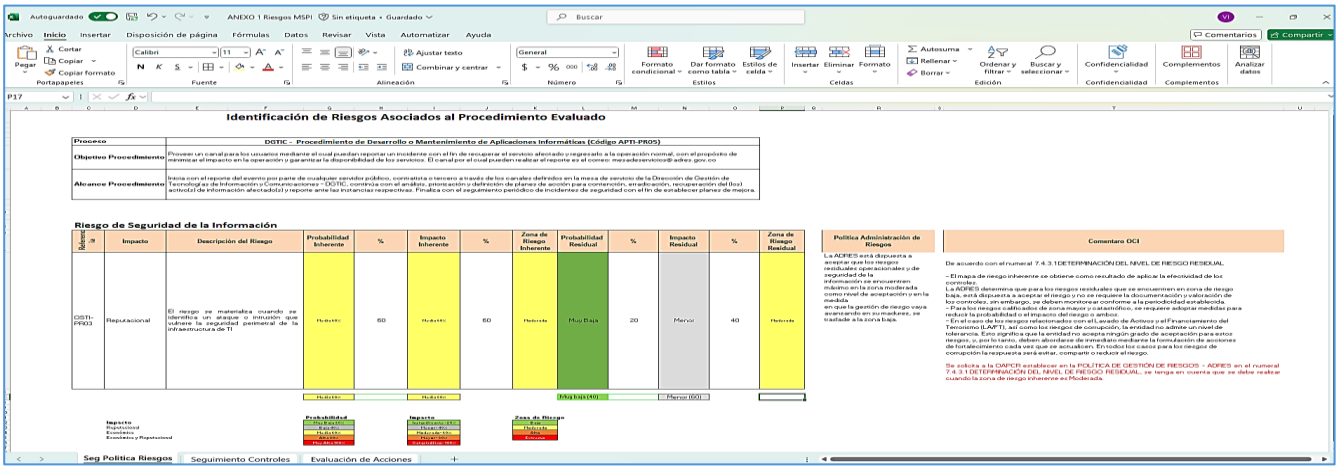
- **Indicadores.**

Se observó a través de la herramienta Eureka que el Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03, de la DGTI**,** no tiene definido indicadores de eficacia, eficiencia y efectividad que permitan monitorear los resultados de medición del procedimiento.

De acuerdo con la mesa de trabajo, la DGTIC tendrá en cuenta en su plan de mejora el riesgo de gestión APTI-RG01 al corte de julio 25 de 2024, correspondiente al Procedimiento Gestión de Incidentes de Seguridad V3 OSTI-PR03,, en el cual se observó que los cinco (5) puntos de control **P.C.,** establecidos en el citado procedimiento, no están asociados al riesgo de gestión APTI-RG01. Así:



Código del riesgo	Identificador	Descripción	Causas	Consecuencias	Procesos	Áreas organizativas	Responsable	Gestor	Subsistema del riesgo
OSTI-RS03	Posibilidad de afectación reputacional por pérdida parcial o total de información, debido a ataques, fallas, alteraciones u omisiones en la seguridad perimetral de la infraestructura de TI	El riesgo se materializa cuando se identifica un ataque o intrusión que vulnere la seguridad perimetral de la infraestructura de TI	* Tecnología - 1. Complementos de seguridad desactualizados en los servicios de TI que preveen terceros. * Procesos - 2. Ausencia u omisión de alertas generadas de mecanismos de monitoreo de herramientas de TI * Procesos - 3. Error o falta de configuración en la seguridad perimetral	* 3. Afectación de imagen institucional * 1. Pérdida parcial o total de la configuración de la plataforma de TI. * 2. Reprocesos en las actividades propias	* Operación y Soporte a las Tecnologías de Información y las Comunicaciones	* Dirección de Gestión de Tecnologías de Información y Comunicaciones	Saul Diaz Olivares	Carlos Felipe Rodriguez Ordoñez	Seguridad de la información



RESPUESTA POR LOS ADUDITADOS

Radicado No.: 20241300570163 Fecha: 2024-11-22 17:03

Respecto de estas observaciones, solicitamos realizar una mesa de trabajo entre la OCI y los responsables de gestionar los procedimientos mencionados y sus riesgos asociados, con el fin de entender estas observaciones, para aclarar las inquietudes y de esta forma la OCI pueda generar las observaciones que se deriven de este entendimiento.

RESPUESTA POR LA OCI

*En cuanto a los procedimientos del proceso Operación y Soporte a las Tecnologías de Información y las Comunicaciones (OSTI), **se recomienda** hacer una revisión de identificación de riesgos asociados a los controles de gestión de riesgo toda vez que los puntos de control OSTI-PR03 están asociados a la política mas no al procedimiento.*

- **POLÍTICA RELACIÓN CON PROVEEDORES**

La ADRES establece las condiciones para la prestación de los servicios, responsabilidades y controles que ayuden a proteger la información involucrada en las relaciones entre la Entidad con sus terceros, frente a interceptaciones, copia, modificación, divulgación y destrucción no autorizada, que puedan afectar los principios de integridad, disponibilidad y confidencialidad de la información.

El objeto de la Política Relación con Proveedores en la ADRES, establece lineamientos, obligaciones y restricciones a los proveedores que presten un servicio o tengan interacción con la información de la ADRES, conservando los principios de disponibilidad, integridad y confidencialidad de la información.

- De acuerdo con lo expuesto se presenta los siguientes documentos que se encuentran en EUREKA y que dan alcance a la política:

Tabla 5. Documentación - Proveedores - EUREKA

Nombre	Código	Tipo	Versión	Fecha versión	Estado
Política Relación con Proveedores	OSTI-PL03	Política	1	29/11/2023 10:46	Activo
Solicitud de Información a Proveedores	GCON-FR19	Formato	2	20/12/2022 23:59	Activo
Generación de Archivo de IPS y o Proveedores Beneficiarios de Giro Directo	VALR-PR30	Procedimiento	2	23/10/2019 0:00	Activo

De acuerdo con la **Tabla 5**, en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) - Relación con Proveedores de Seguridad Digital, no se cuenta con un procedimiento o manual que integre los siguientes lineamientos que dan alcance a la política.

- **Planificación de las relaciones con Proveedores:** Establecer un plan de relación con proveedores que documente la decisión adoptada por el nivel directivo de iniciar la contratación de un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación.

  Gestionar con éxito la seguridad de la información dentro del proceso de planeación de la relación con los proveedores de productos o servicios de seguridad de la información.

- **Selección de proveedores:** Planificar la selección de los proveedores de productos o servicios de seguridad de la información.

  Gestionar con éxito la seguridad de la información dentro del proceso de selección de proveedores de productos o servicios de seguridad de la información.

- **Negociación de Acuerdos con Proveedores:** Gestionar la seguridad de la información en el proceso en el proceso de negociación de acuerdos con proveedores.

  Gestionar con éxito la seguridad de la información dentro del proceso de negociación de la relación con los proveedores de productos o servicios de seguridad de la información.

- **Gestión de relaciones con proveedores:** Mantener la seguridad de la información durante el período de ejecución de la relación con el proveedor.

  Gestionar con éxito la seguridad de la información durante la relación con el proveedor de productos o servicios de seguridad de la información.

- **Proceso de terminación de la relación con el proveedor:** Planificar el cierre contractual con los proveedores de productos o servicios de seguridad de la información.

Gestionar con éxito y de manera segura la terminación de la relación con el proveedor de productos o servicios de seguridad de la información garantizando la continuidad de la operación.

De acuerdo con lo anterior es importante revisar el procedimiento *Desarrollo o Mantenimiento de Aplicaciones Informáticas* si estos lineamientos si requieren articularse y formar un solo procedimiento de Adquisición, Desarrollo y Mantenimiento.

Observación 4:

De acuerdo con la **Tabla 5**, se puede verificar que la Entidad no cuenta con un procedimiento o manual que integre la Planificación de las relaciones con Proveedores, Selección de proveedores, Negociación de Acuerdos con Proveedores, Gestión de relaciones con proveedores y Proceso de terminación de la relación con el proveedor. en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) - Relación con Proveedores de Seguridad Digital

Condición:

De acuerdo con la Política Relación con Proveedores, según la **Tabla 5**, se puede verificar que la Entidad no cuenta con un procedimiento o manual que integre la Planificación de las relaciones con Proveedores, Selección de proveedores, Negociación de Acuerdos con Proveedores, Gestión de relaciones con proveedores y Proceso de terminación de la relación con el proveedor. en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) - Relación con Proveedores de Seguridad Digital

Criterio:

Lo anterior da incumplimiento a la Resolución Número 00500 de Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" que establece lineamientos que deben ser cumplidos por los responsables para la gestión y clasificación de los Activos de Información en la ADRES, sujetos a la Política General de Seguridad y Privacidad de la Información de la Entidad.

Causa:

De la revisión efectuada por parte de la OCI, se observó que no se cuenta con un procedimiento o manual que de alcance a los lineamientos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI) - Relación con Proveedores de Seguridad Digital según la ARTÍCULO 6. La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. Los sujetos obligados deben determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades: numera 8 Realizar un análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros.

Consecuencia:

En consecuencia, y de acuerdo con lo establecido en la Resolución Número 00500 de Marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", se solicita a la OAPCR y a la DGTIC que el incumplimiento de la formulación de acciones de fortalecimiento para la Política Relación con Proveedores V1 – Noviembre 2023, conlleva implicaciones, estas incluyen un aumento significativo en la vulnerabilidad de la organización a actividades de corrupción e incumplimiento de los mandatos regulatorios. Así mismo, este incumplimiento podría generar posibles sanciones legales y afectar la reputación de la Entidad.

VERIFICACION MAPA DE RIESGOS Y CONTROLES

De acuerdo con la Guía para la Administración del Riesgo y el diseño de controles en Entidades públicas Versión 6., se informa que dado el resultado de la **observación 4** no se puede realizar la verificación de controles de riesgo hasta que no se de alcance a un procedimiento con respecto a la relación con proveedores.

RESPUESTA POR LOS ADUDITADOS

Radicado No.: 20241300570163 Fecha: 2024-11-22 17:03

Respecto de nuestro Modelo de Seguridad y Privacidad de la Información (MSPI), la ADRES cuenta con un Manual de Políticas específicas de seguridad de la información, que se complementa con un plan de control operacional en donde se incluyen los componentes de la norma ISO/27001 como guía de buena práctica internacional y un plan de gestión de riesgos de seguridad de la información identificados en la Entidad. No obstante, los lineamientos definidos en el MSPI se gestionan con la valoración del nivel de madurez del Modelo a través de un instrumento diseñado por MINTIC que la Entidad se tiene actualmente implementado para este fin.

La OAPCR no ha definido un procedimiento asociado al Modelo de Seguridad y Privacidad de la Información, toda vez que con los mecanismos acá mencionados se gestionan adecuadamente.

RESPUESTA POR LA OCI

En cuanto a los procedimientos del proceso Operación y Soporte a las Tecnologías de Información y las Comunicaciones (OSTI), **se recomienda** hacer una revisión de identificación de riesgos asociados a los controles toda vez que algunos puntos de control están asociados a la política mas no al procedimiento o están sin asociar a ningún lineamiento. (ver mapa de riesgo de seguridad de la información de la herramienta Eureka, código de riesgo OSTI.

- **POLÍTICA DE USO DEL SERVICIO DE CORREO ELECTRÓNICO CORPORATIVO**

La ADRES presta el servicio de correo electrónico mediante la herramienta Microsoft Exchange Online, sobre la cual se podrán asignar buzones de correo electrónico a los miembros de los diferentes grupos de interés de la Entidad, respetando los lineamientos consignados en esta política y de conformidad con el procedimiento de control de acceso. Esta Política y cada uno de sus componentes son sujetos a la mejora continua a través de los planes originados en los procesos de evaluación o de auditoría.

El objetivo es establecer las responsabilidades, lineamientos y prácticas que deben cumplir los usuarios, administradores y personal de soporte técnico del servicio de correo electrónico corporativo con el fin

promover el debido uso, así como proteger la infraestructura y la información contra posibles ciberataques a través de este medio de comunicación y de colaboración.

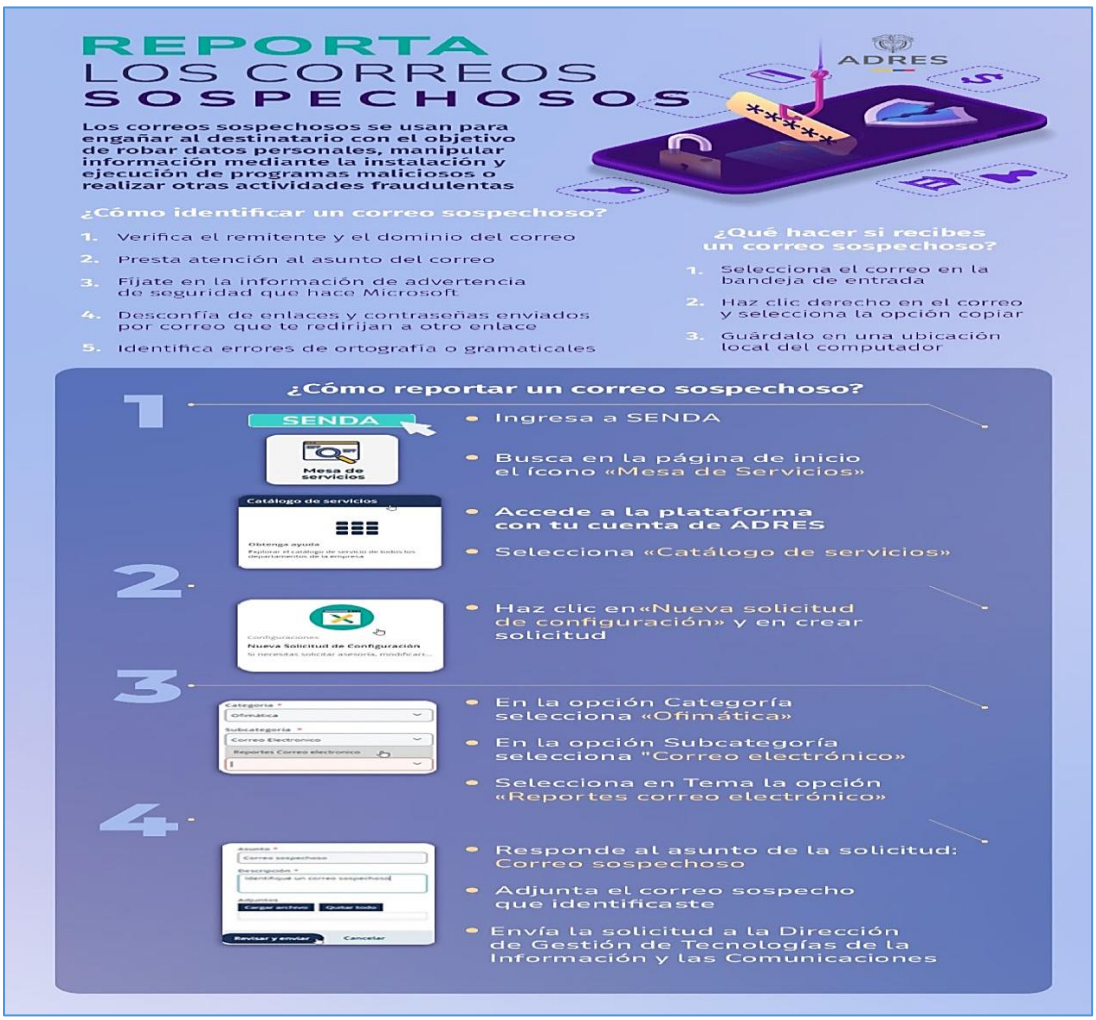
De acuerdo con lo expuesto se presenta los siguientes documentos que se encuentran en EUREKA y que dan alcance a la política:

Tabla 4. Documentación - Correo - EUREKA

Nombre	Código	Tipo	Versión	Fecha versión	Estado
Servicio de Correo Electrónico Corporativo	OSTI-PL02	Política	1	23/11/2023 12:07	Activo

De acuerdo con la **Tabla 6**, según la Política de Servicio de Correo Electrónico Corporativo no se evidencia un manual para la creación de una cuenta de correo electrónico.

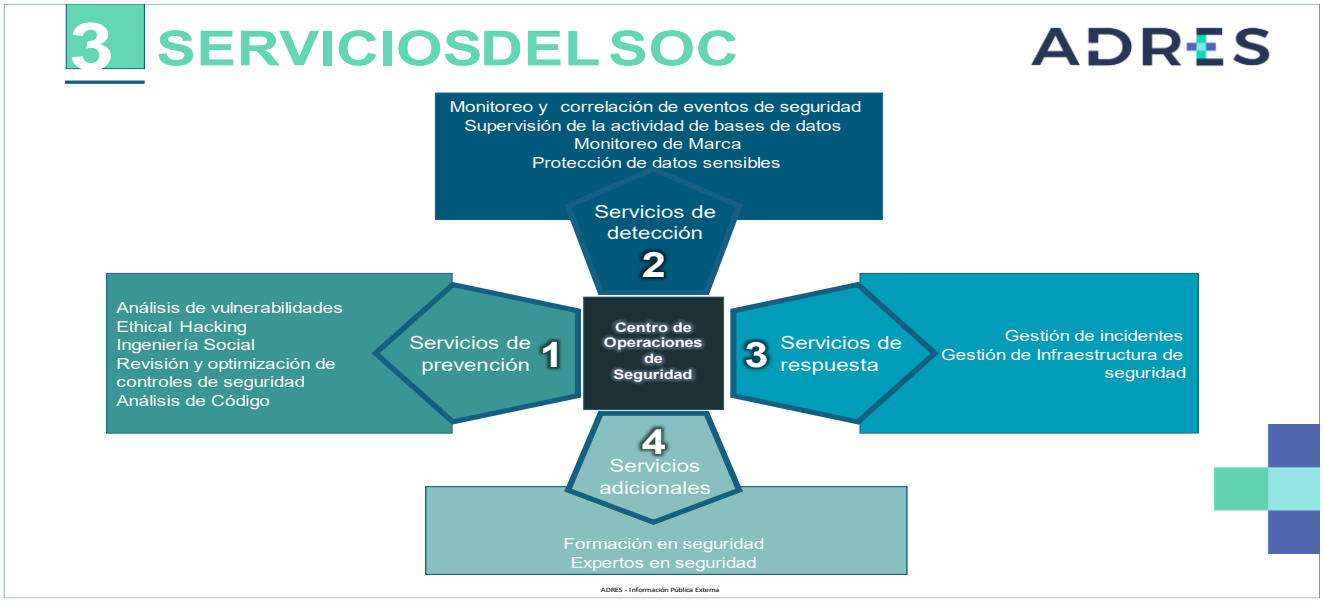
Por otro lado para dar alcance a la Política de Correo Electrónico, la Entidad cumple ya que cuenta con diferentes mecanismos que hacen que la Entidad este al tanto del buen uso del correo electrónico y uno de esos se verifican así:



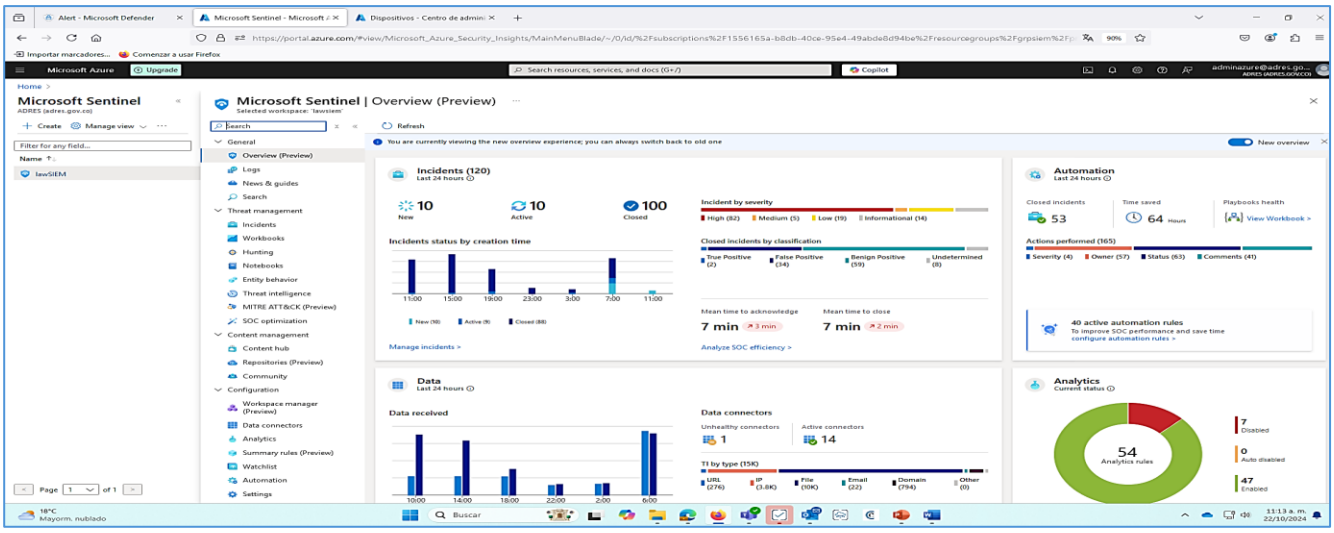
MUESTRA - UT SOC ADRES 2023

De acuerdo con el contrato **ADRES-CTO-868-2023** entre **UT SOC ADRES 2023 y INDRA COLOMBIA S.A.S**, y la participación **DEXTERA S.A.S.,** con el objeto Prestar el Servicio de Centro de Operaciones de Seguridad para la ADRES (SOC). la Entidad cuenta con una herramienta con centro de operaciones de seguridad (SOC) que mejora las capacidades de detección, respuesta y prevención de amenazas de seguridad cibernética al unificar y coordinar todas las tecnologías y operaciones de seguridad cibernética.

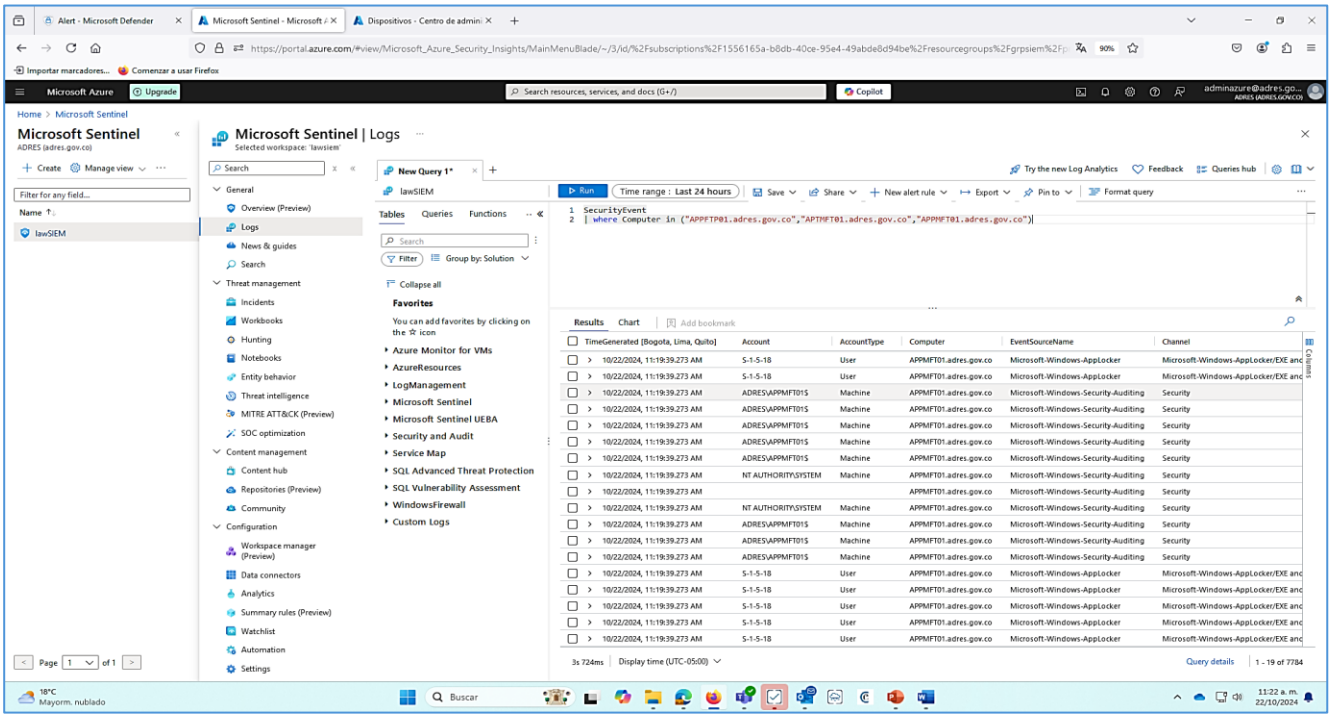
A continuación como muestra y alcance al cumplimiento de las políticas se realizó la siguiente verificación en la herramienta SOC con el oficial de seguridad de la DGTIC así:



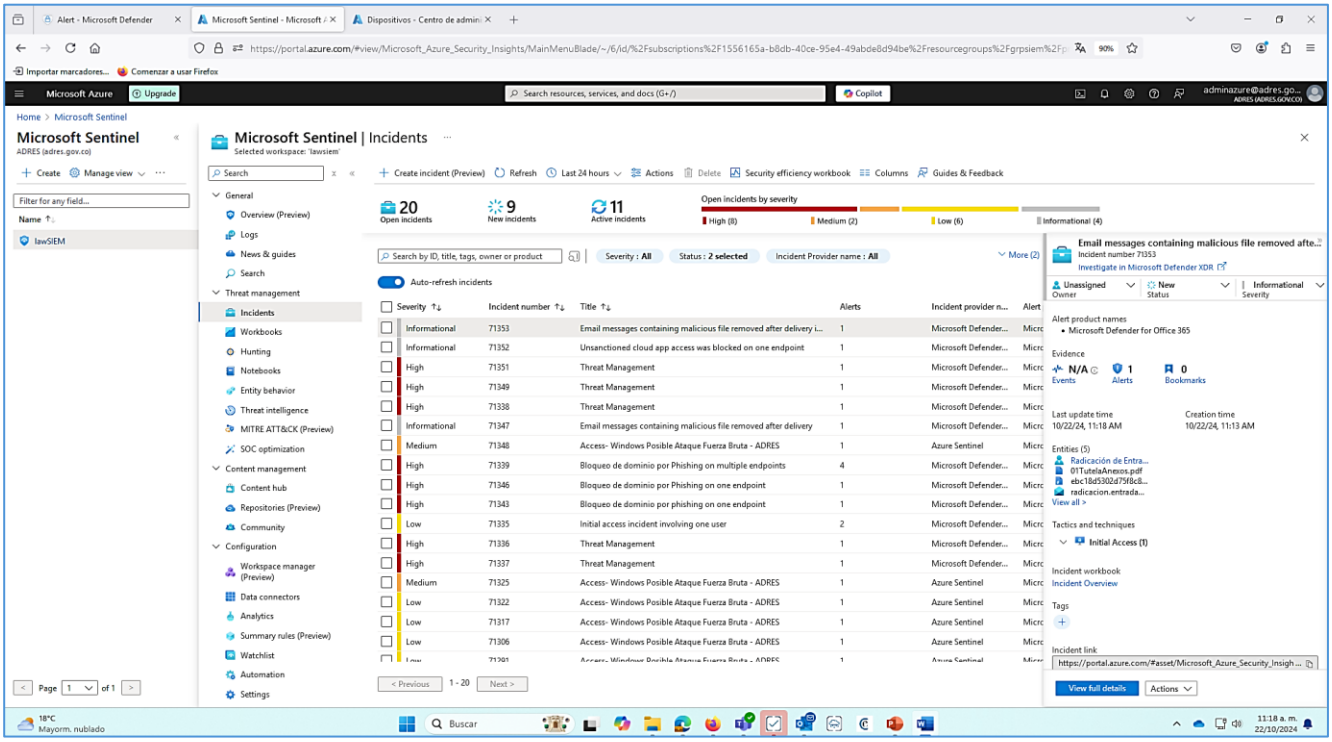
- **Correlacionador de eventos – SIEM – Azure Sentinel**



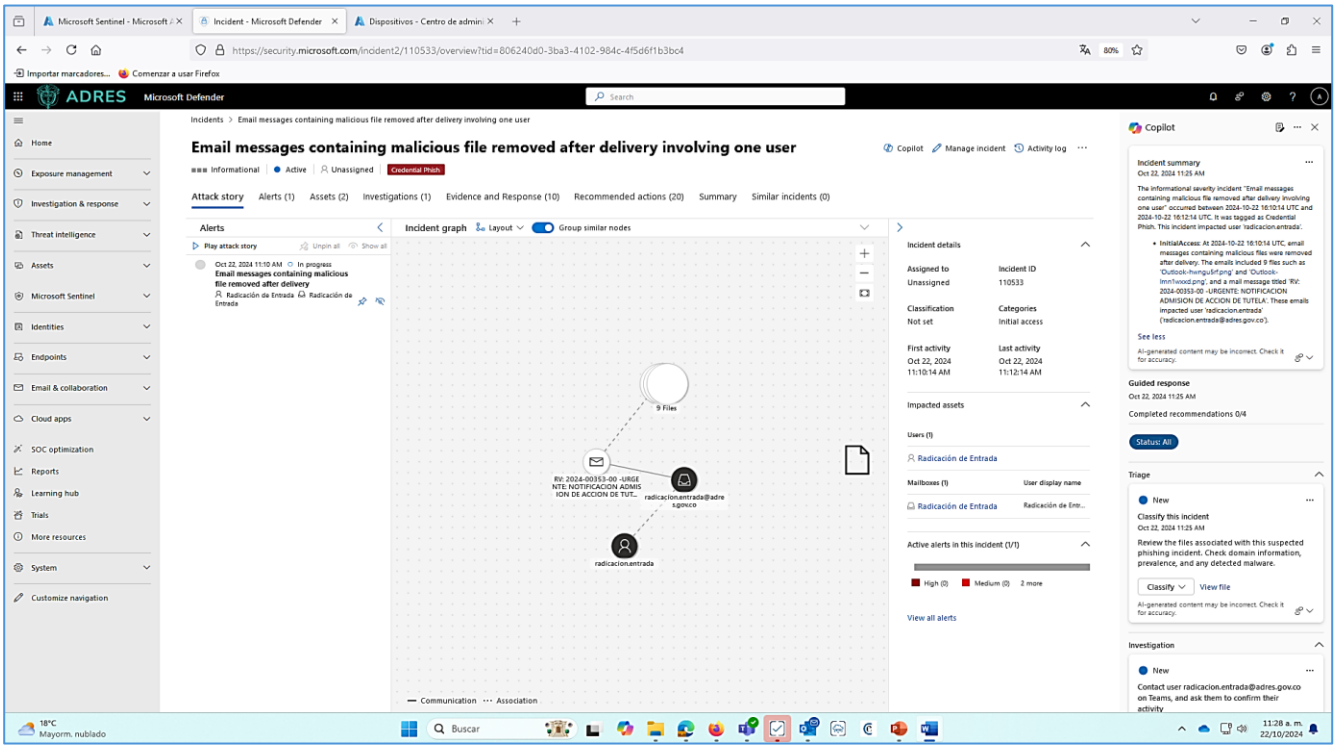
- **Consulta de logs**



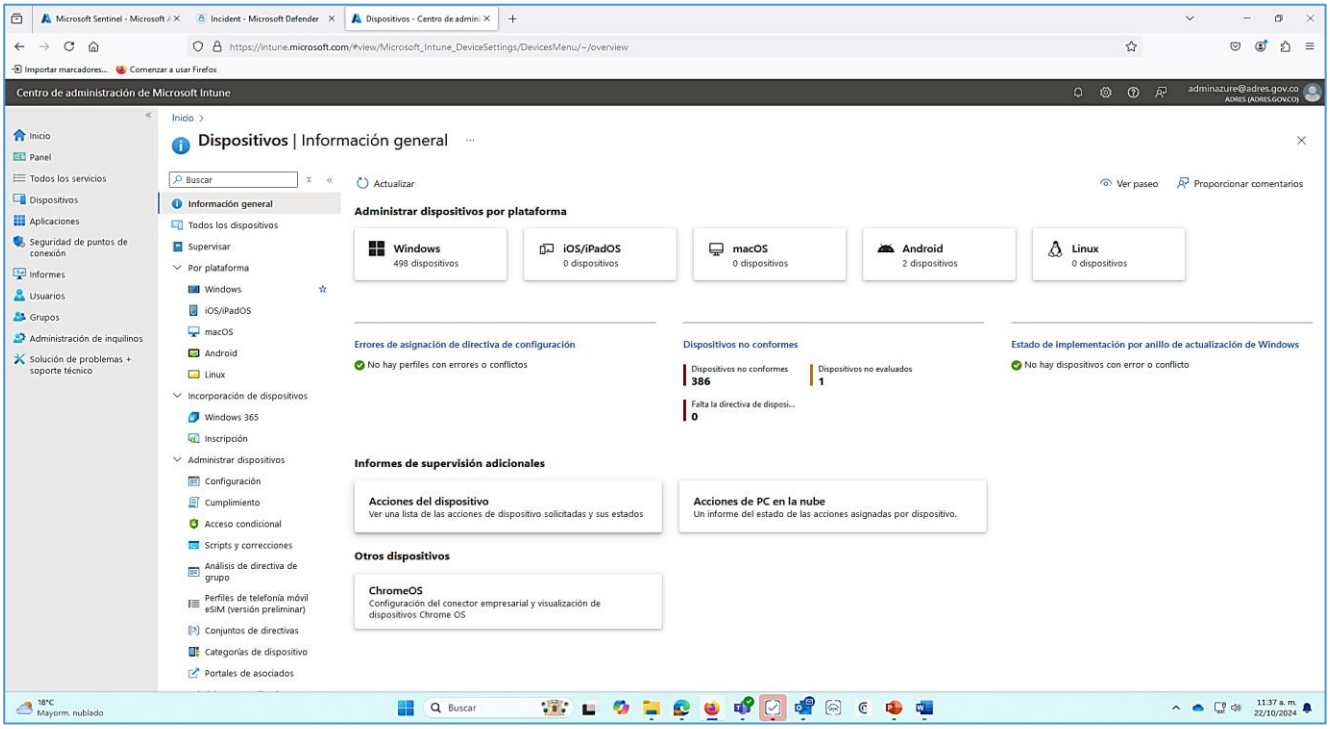
- **Eventos**



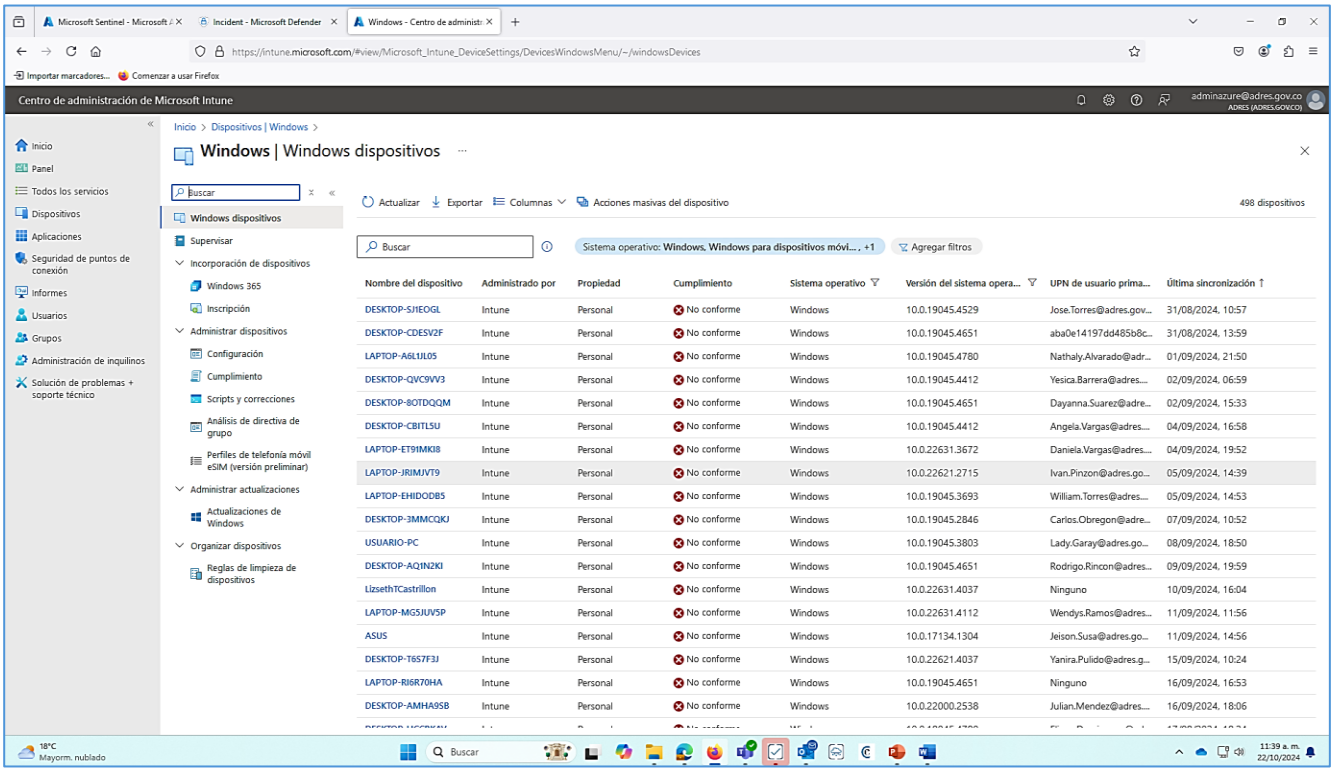
- **Investigación a través Microsoft defender**



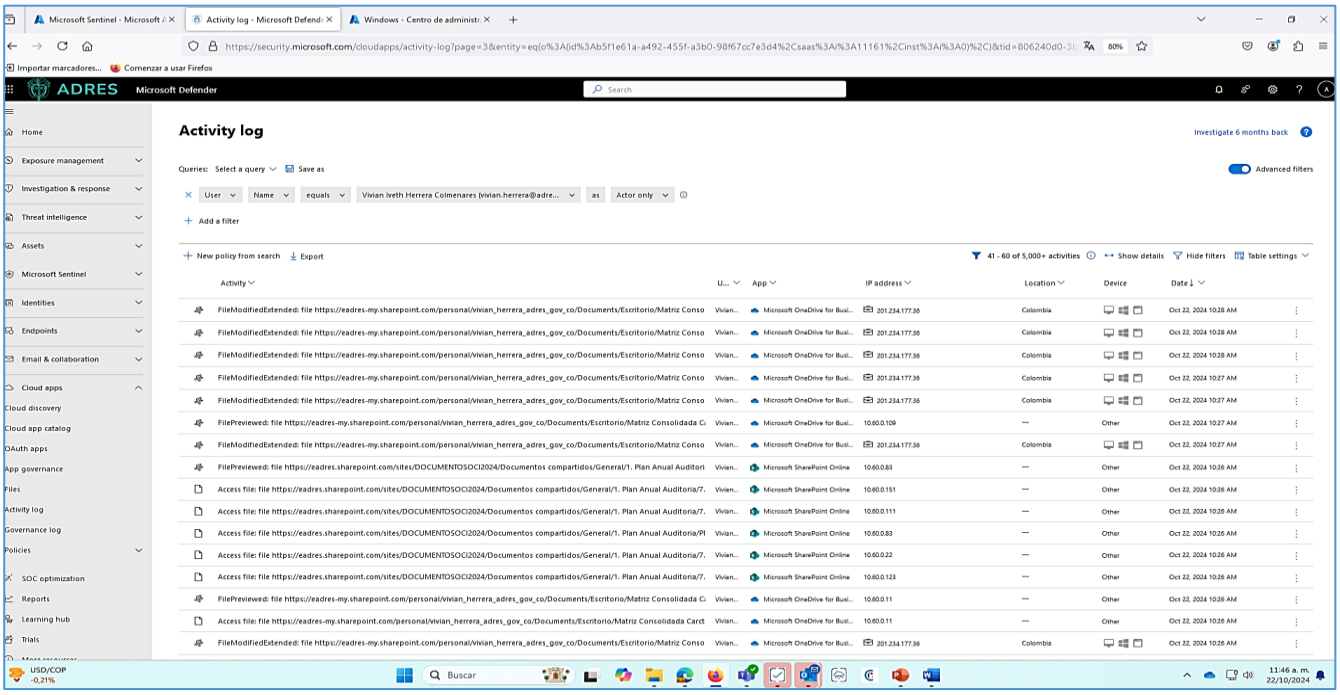
- **Gestión de dispositivos móviles**



- **Dispotivos personales**



- **Logs de actividad**



2. CONCLUSIONES

Del seguimiento a la Implementación de las Políticas (i)Protección de Datos Personales – (ii)Política General de Seguridad y Privacidad de la Información – (iii) Política de Relación con Proveedores – (iv)Política servicio de correo electrónico corporativo y su aplicabilidad con los procedimientos, a continuación se realizan las siguientes conclusiones:

Política de protección de datos personales

De la Política de Protección de Datos Personales V2 – 29 de diciembre 2022 se concluye que en conformidad con la revisión que realizó la OCI a la Resolución Número 3486 de 2018, Resolución Número 0000797 de 2022 , Resolución 798 de 2022 y Resolución Número 73194 de 2022, la OAPCR debe realizar lo pertinente en la designación del oficial de datos personales quien en sus funciones dará el alcance y cumplimiento a la formulación e implementación de lineamientos según la normativa vigente**,** por lo anterior es necesario que se establece un plan de mejora. **Observación 1**

Política de Seguridad y Privacidad de la información

De la Política General de Seguridad y Privacidad de la Información V4 – 29 de diciembre 2022 En relación con el oficial de ciberseguridad, se evidenció que las funciones de este están establecidas en el Manual APTI-MA01 Políticas Específicas de Seguridad y Privacidad de la Información en el numeral *8.4 Unidad de seguridad de la información y la ciberseguridad*, es competencia de la Dirección de la Adres así:

- ✓ *8.4 Unidad de seguridad de la información y la ciberseguridad*

  La Junta Directiva de la ADRES, será la responsable de aprobar esta Política y la autorización de sus modificaciones.
  La Dirección de la ADRES, asigna las funciones relativas a la Seguridad de la Información y Ciberseguridad al Oficial o Responsable de Seguridad de la Información quien tendrá a cargo las funciones relativas del rol, lo cual incluye la supervisión de todos los aspectos inherentes tratados en el presente documento, el control del ***cumplimiento de la Política de Seguridad de la Información y Ciberseguridad,*** *así como garantizar que las políticas específicas, procesos, procedimientos y/o controles que se deriven de esta estén alineados con la Política y ésta con las estrategias y modelos del negocio.*

Por lo anterior las funciones relativas a seguridad de la información y ciberseguridad está a cargo del Oficial de cumplimiento, cuya designación está establecida en la resolución 0082303 del 2024 al servidor público Rodolfo Oswaldo Uribe *"Por la cual se designa el Oficial de Cumplimiento y secretario técnico del Comité Institucional de Riesgo de la Administradora de los Recursos del Sistema General de Seguridad Social En Salud – ADRES"*

1. RECOMENDACIONES

De las políticas evaluadas y analizadas se realizan las siguientes recomendaciones:

Política de Seguridad y Privacidad de la información

1. En cuanto a los procedimientos del proceso Operación y Soporte a las Tecnologías de Información y las Comunicaciones (OSTI), **se recomienda** hacer una revisión de identificación de riesgos asociados a los controles toda vez que algunos puntos de control están asociados a la política mas no al procedimiento o están sin asociar a ningún lineamiento. (ver mapa de riesgo de seguridad de la información de la herramienta Eureka, código de riesgo OSTI.

Política Relación con Proveedores

2. En cuanto a la Política de Relación con Proveedores y el manual APTI-MA01_Políticas específicas de Seguridad y Privacidad de la Informacíon V4.pdf se evidenció que esta se encuentran establecidas, sin embargo no tienen asociado un procedimientos, ni identificación de eventos de riesgos que den los lineamientos para su implementación, por lo anterior se recomienda al momento de establecer los procedimientos tener en cuenta la guía Relación con Proveedores de Seguridad Digital.

3. Se recomienda la OAPCR y DGTIC, realizar campañas de socialización y sensibilización a la Entidad frente a las políticas de:

   - Política de Protección de Datos Personales V2 – 29 de diciembre 2022
   - Política General de Seguridad y Privacidad de la Información V4 – 29 de diciembre 2022
   - Política Relación con Proveedores V1 – noviembre 2023

2. RESPONSABLES DE LA AUDITORÍA			
Nombre	**Firma**	**Proceso**	**ROLES Y RESPONSABILIDADES** (Auditor líder, Auditado, Auditor, Observador, Jefe OCI)
Vivian Iveth Herrera Colmenares	Iniciales de Vivian Iveth Herrera Colmenares el 19/12/2024 a las 18:26:14 COT	**CEGE**	**Auditora**

Fecha de Revisión: 19 de diciembre 2024

Fecha de Aprobación: 19 de diciembre 2024

Cordialmente,

Firmado por FLOREZ PARDO DEISY CAROLINA
Fecha: 19/12/2024 18:28:21 COT

DEISY CAROLINA FLOREZ PARDO
Jefe Oficina de Control Interno

Elaboró: Vivian Iveth Herrera Colmenares – Auditora TIC-OCI

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS					
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**ELABORADO POR:**	**REVISADO POR:**	**APROBADO POR:**
01	*20 de abril de 2018*	Versión Inicial	Lizeth Lamprea Asesor OCI	Diego Santacruz Jefe de la OCI	Diego Santacruz Jefe de la OCI
02	*25 de noviembre de 2019*	Estandarización Tipo, Tamaño Letra. Márgenes. Incorporación de responsables Se ajusto el nombre del formato	Lizeth Lamprea Asesor OCI	Diego Santacruz Jefe de la OCI	Diego Santacruz Jefe de la OCI
03	*20/05/2022*	Se suprimen firmas mecánicas y se incluye firma digital	Lizeth Lamprea Asesor OCI	Diego Santacruz Jefe de la OCI	Diego Santacruz Jefe de la OCI