AGENCIA NACIONAL DE DEFENSA JURIDICA DEL ESTADO

INFORME DE AUDITORÍA AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN A-P-GTI-01-2023

Septiembre 2023
Oficina de Control Interno
Elaborado Por: Andrés Mauricio Cruz Vargas
Aprobado por: Marcela Villate Tolosa

1. Introducción:

La Oficina de Control Interno de la Agencia Nacional de Defensa Jurídica del Estado, en el desarrollo de su Plan Anual de Auditorias 2022 – 2023, practicó la auditoría al plan de Seguridad y Privacidad de la Información, con el objetivo de Verificar la información, procedimientos, procesos y manuales que comprenden y hacen parte del Modelo de Seguridad y Privacidad de la Información – MSPI.

En el marco de la Auditoría de verificó:

- Madurez del MSPI.
- Diagnóstico del Plan de Continuidad del Negocio BPC y Plan de Recuperación de Desastres DRP
- Identificación bases de datos personales

Dicha auditoria se efectuó del 01 al 31 de agosto de 2023 y sus resultados se presentan a continuación.

2. Desarrollo del informe:

El análisis realizado por parte de la Oficina de Control Interno a la madurez al Modelo de Seguridad y Privacidad de la Información – MSPI, se realizó tomando como base la herramienta que creó el Ministerio de Tecnologías de la Información y las Comunicaciones "Instrumento de Evaluación del MSPI", el cual tiene como fin poder identificar el nivel de madurez en las entidades del estado, permitiendo así establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las mismas.

Así las cosas, se realizó el análisis y validación documental (normas, procedimientos, políticas, manuales, leyes, entre otros), por lo cual se presenta a continuación los resultados obtenidos para cada uno de los dominios incluidos en el Instrumento de evaluación del MSPI.

– MADUREZ DEL MSPI.

La Oficina de Control Interno, realizó el análisis y verificación documental registrada, obteniendo los siguientes resultados:

Tabla No. 1 Nivel de Madurez del MSPI

INFORMACIÓN SOLICITADA	DOCUMENTO ENTREGADO	COMENTARIOS OCI
Tipo de entidad (Nacional, Territorial A, Territorial B o C)	https://www.defensajuridica.gov.co/Paginas/Home.aspx	Conforme con la información suministrada, se evidencia que cada uno de los ítems registrados cumple con lo estipulado.
Misión	http://www.defensajuridica.gov.co/agencia/quienessomos/Paginas/mision-vision.aspx	
Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.	Contexto Interno: Procesos Áreas Colaboradores	
	Contexto Externo: Proveedores	

INFORMACIÓN SOLICITADA	DOCUMENTO ENTREGADO	COMENTARIOS OCI
	Normatividad Vigente.	
Mapa de Procesos.	https://www.defensajuridica.gov.co/agencia/quienessomos/Paginas/mapa_procesos.aspx	
Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces.	https://www.defensajuridica.gov.co/agencia/quienessomos/Paginas/organigrama.aspx.	
Políticas de seguridad de la información formalizada y firmada.	DE-M-02 Manual de Políticas de Gestión y Desempeño Institucional de la Agencia.	
Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	Resolución 095 de 26 de febrero 2018.	De conformidad con el numeral 2 del artículo 2° "Conformación del nuevo Sistema Integrado de Gestión Institucional - SIGI", esta Oficina constató la asignación de los responsables de la implementación, sostenimiento y mejora de los diferentes SIGI, entre los cuales se encuentra el SGSPI "Subsistema de Gestión de Seguridad Privacidad de la Información – SGSPI".
Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección.	Plan y estrategia de transición de Ipv4 a Ipv6 fue aprobado por la alta dirección – Coexistencia de IPv4 e Ipv6.	De conformidad con la Guía de Transición de Ipv4 a Ipv6 de Mintic, se describen tres fases: Planeación, Implementación, Pruebas de funcionalidad. Así las cosas, esta Oficina constató en el documento remitido, cada uno de los apartes descritos en la guía mencionada.
Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información).	Objetivos: Orientar los lineamientos establecidos para el Subsistema de Seguridad y Privacidad de la Información de acuerdo con la estrategia de negocio y la regulación vigente.	Conforme con la información suministrada, se evidencia que cada uno de los ítems registrados cumple con lo estipulado.
Procedimientos de control documental del MSPI.	Se copia enlace de consulta: https://andj.darumasoftware.com/app.php/staff/portal/documents?form_filter%5Bdepartments_list%5D=11&form_filter%5B_csrf_token%5D=cbf3698bfc9eda723e2f415c858f0682.	
Metodología de Gestión de riesgos.	https://andj.darumasoftware.com/app.php/staff/document/viewPublic?index=707.	
Riesgos identificados y valorados de acuerdo con la metodología.	Se vienen identificando riesgos de manera periódica.	
Planes de tratamiento de los riesgos.	Se documentaron los planes de tratamiento de riesgos.	
Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información.	Clausulas establecida en el Manual de Funciones y en Contratos para Seguridad de la Información.	
Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad.	Solicitud de antecedentes Policía Nacional, Contraloría y Procuraduría.	De conformidad con el procedimiento "GC-P-10 - Contratación Directa", se evidencia el procedimiento el cual indica el diligenciamiento del formato "GC-F-34 Constancia de verificación de

INFORMACIÓN SOLICITADA	DOCUMENTO ENTREGADO	COMENTARIOS OCI
		antecedentes en proveedores extranjeros" para toda persona jurídica extranjera y del representante legal, o apoderado, o socio facultado para contratar.
Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	GTI-PN-01 PLAN DE CAPACITACION DE TI	Conforme con la información suministrada, se evidencia que cada uno de los ítems registrados cumple con lo estipulado.
Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información.	Aplica Código Único Disciplinario (Ley 734 de 2002) y el Estatuto Anticorrupción (Ley 1474 de 2011).	
Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección.	Matriz de activos de información.	De conformidad con la información suministrada por parte de la OASTI, se evidenció un sistema de información en el cual se realiza la gestión del inventario de activos de información.
Inventario de áreas de procesamiento de información y telecomunicaciones.		
Diagrama de red de alto nivel o arquitectura de TI.	Diagramas técnicos.	Conforme con la información suministrada por parte de la OASTI, se evidenció la existencia del documento "Diagrama Infraestructura" en el cual se detalla a alto nivel la infraestructura de la entidad.
Inclusión de la seguridad de la información en la gestión de proyectos.	En su momento era un tema que no era tenido en cuenta (2021) pero después del 2022 con el PETI se incorporó.	Según lo dispuesto en el PETI de los años 2022 y 2023, se incorpora la seguridad y privacidad de la información.
Inventario de partes externas o terceros a los que se transfiere información de la entidad.	Se adjunta documento GUÍA PARA REALIZAR EL PROCESO DE CARACTERIZACIÓN DE CIUDADANÍA Y GRUPOS DE VALOR DE LA AGENCIA donde en el capítulo 4. CONCLUSIONES Y RECOMENDACIONES se listan los grupos de interés de la Agencia y estos hacen parte del alcance del MSPI (Modelo de Seguridad y Privacidad de la Información).	Conforme con la información suministrada, se evidencia el documento "Contacto con Autoridades y Grupos de Interés en Seguridad", cumpliendo con lo estipulado.
Formato de acuerdo de transferencia de información.	Documento en construcción	Al respecto y conforme con lo manifestado por la OASTI, esta Oficina **recomienda** generar el formato de acuerdo de colaboración para el intercambio de información.
Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden.	Se adjunta listado de proveedores (personas naturales) que acceden a nuestros sistemas de información.	Conforme con la información suministrada, se evidencia el documento "Listado proveedores", cumpliendo con lo estipulado.
Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	Reporte de incidentes	De conformidad con la información suministrada por parte de la OASTI, se evidenció dos documentos en cuestión.
Plan de continuidad de la Entidad aprobado	El plan fue documentado y aprobado en el 2022.	Conforme con el documento remitido por parte de la OASTI, "Documento de

INFORMACIÓN SOLICITADA	DOCUMENTO ENTREGADO	COMENTARIOS OCI
		pruebas, ejecución y resultados de DRP y BCP", esta Oficina no tiene observaciones a lugar.
Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	Normograma	Al respecto, el normograma se evidencia ubicado en la página web institucional y en el Sistema de Gestión Documental – DARUMA.
Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad.	Plan de auditorías Control Interno.	Al respecto, en la página web institucional se encuentra el plan de auditorías del año 2013 a la fecha.
Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.	Se copia enlace de consulta: https://andj.darumasoftware.com/app.php/staff/portal/documents?form_filter%5Bdepartments_list%5D=11&form_filter%5B_csrf_token%5D=cbf3698bfc9eda723e2f415c858f0682.	Al respecto, los documentos en cuestión se evidencian en el Sistema de Gestión Documental – DARUMA.
Declaración de aplicabilidad	Declaración de aplicabilidad 2023.	Conforme con la información suministrada, se evidencia el documento "Declaración Aplicabilidad_2023", cumpliendo con lo estipulado.
Aceptación de los riesgos residuales por parte de los dueños de los riesgos.	Aprobación por los dueños y CIGD.	Se evidencian dos actas del Comité Institucional de Gestión y Desempeño, correspondientes a los años 2022 y 2023, en los cuales se realiza la aprobación de aceptación del riesgo residual.
Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Plan de Seguridad.	Conforme con la información suministrada, se evidencia el documento "Plan de Seguridad y Privacidad de la Información", cumpliendo con lo estipulado.
Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	Aprobación por los dueños y CIGD.	Se evidencian dos actas en las cuales el Comité Institucional de Gestión y Desempeño, correspondientes a los años 2022 y 2023.
Documento con el plan de auditorías internas y resultados, de acuerdo con lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	Plan de auditorías Control Interno.	Al respecto, en la página web institucional ANDJE se encuentra el plan de auditorías del año 2013 a la fecha.
Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	Aprobación por los dueños y CIGD.	Se evidencian dos actas en las cuales el Comité Institucional de Gestión y Desempeño, correspondientes a los años 2022 y 2023, en los cuales se realiza la aprobación de aceptación del riesgo residual.
Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	Plan de seguridad.	Conforme con la información suministrada, se evidencia el documento "Plan de Seguridad y Privacidad de la Información", cumpliendo con lo estipulado.

INFORMACIÓN SOLICITADA	DOCUMENTO ENTREGADO	COMENTARIOS OCI
Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.	Plan de auditorías Control Interno.	Al respecto, en la página web institucional ANDJE se encuentra publicado el documento de plan de auditorías desde el año 2013.

– VALIDACIÓN DE CONTROLES "MSPI"

La verificación y posterior evaluación de cumplimiento de los controles diligenciados en el Instrumento de Evaluación del MSPI, se llevará a cabo conforme la siguiente tabla:

Tabla No. 2 Tabla de Valoración de los Controles MSPI

VALORACIÓN	DESCRIPCIÓN DE LA EVALUACIÓN
Cumple	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Cumple Parcialmente	Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
No Cumple	La Entidad ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.

– VALIDACIÓN DE CONTROLES “MSPI”

Tabla No. 3. Validación Controles MSPI.

A.5. – POLITICAS DE LA SEGURIDAD **A.5.1 – Orientación de la dirección para la gestión de la seguridad de la información**				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.5.1.1	Políticas para la seguridad de la información.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Cumple	Se evidenció el documento “Manual de Políticas de Gestión y Desempeño Institucional de la Agencia”.
A.5.1.2	Revisión de las Política de Seguridad de la Información.	Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	Cumple	Se evidenció dos documentos “Manual de Políticas de Gestión y Desempeño Institucional de la Agencia” de los años 2021 y 2022.
A.6. – ORGANZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN **A.6.1 – Organización Interna**				
ANEXO		CONTROL	VALORACIÓN	**COMENTARIOS OCI**
A.6.1.1	Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Cumple parcialmente	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política seguridad para los colaboradores en la cual se indican lineamientos para los colaboradores sean responsables con la seguridad de la información, en el cual se indican: “*Todos los colaboradores de la Agencia deben cumplir con lo establecido en el documento de Roles y Responsabilidades de Seguridad de la Información”*. **Sin embargo, dicho documento a la fecha del presente informe no se encuentra en desarrollo.**
A.6.1.2	Separación de deberes.	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	Cumple parcialmente	Se identifica el documento [GC-M-01] MANUAL DE CONTRATACION - V7, el cual se imparten actividades en la planeación contractual a miras de evitar el conflicto de interés. **Sin embargo, no se evidenció procedimiento que permita la segregación de responsabilidades**.
A.6.1.3	Contacto con las autoridades.	Se deben mantener contactos apropiados con las autoridades pertinentes.	Cumple	

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.6.1.4	Contacto con grupos de interés especial.	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	Cumple	Se evidenció documento "Contacto con Autoridades y Grupos de Interés en Seguridad", el cual incluye los principales contactos de interés.
A.6.1.5	Seguridad de la Información en la gestión de proyectos.	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Cumple	Se identifica que el control en mención se describe a nivel contractual, cláusula de seguridad.
A.6.2 – Dispositivos móviles y teletrabajo.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.6.2.1	Política para dispositivos móviles	Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles	Cumple	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política 6.4.7 para dispositivos móviles.
A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Cumple	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política 6.4.3 para acceso remoto. Por otra parte, conforme con el Procedimiento de Teletrabajo - GH-P-09, esta Oficina realizó un muestreo simple de cuatro casos (29969, 29103, 29102, 28741) con el fin de verificar el cumplimiento con lo dispuesto en registrar el formato de inscripción a Teletrabajo GH-F-43 y como resultado se obtuvo cumplimiento en lo estipulado.
A.7 – SEGURIDAD DE LOS RECURSOS HUMANOS **A.7.1 – Antes de asumir el empleo**				
ANEXO		CONTROL	VALORACIÓN	**OBSERVACION OCI**
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos	Cumple	De conformidad con el procedimiento "GC-P-10 - Contratación Directa", donde se indica el diligenciamiento del formato "GC-F-34 Constancia de verificación de antecedentes en proveedores extranjeros" para toda persona jurídica extranjera y del representante legal, o apoderado, o socio facultado para contratar. Al respecto, se realizó la validación documental de tres contratos por prestación de servicios 001, 055 y 084 de 2023, evidenciando que los contratos tienen la validación de antecedentes y responsabilidades. Así las cosas, se obtuvo cumplimiento en lo estipulado.
A.7.1.2	Términos y condiciones de empleo.	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Cumple	

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.7.2 Durante la ejecución del empleo				
A.7.2.1	Responsabilidades de la dirección.	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Cumple	Conforme con la Resolución 095 de 26 de febrero 2018, numeral 2 del artículo 2 "Conformación del nuevo Sistema Integrado de Gestión Institucional - SIGI", esta Oficina constató la asignación de los responsables de la implementación, sostenimiento y mejora de los diferentes SIGI, entre los cuales se encuentra el SGSPI "Subsistema de Gestión de Seguridad Privacidad de la Información – SGSPI".
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	Cumple	Los documentos "Plan Institucional de capacitación" de los años 2022 y 2023 en el cual se llevaron a cabo varias capacitaciones orientadas a la seguridad de la información. Así las cosas, esta Oficina realizó una muestra de cuatro capacitaciones realizadas durante los años en cuestión así: • Charla Seguridad _Practicas seguras trabajo en casa. • Charla Seguridad de la Información _ Higiene Digital. • Charla Seguridad de la Información _Riesgos en el Mundo Virtual. • Cyberseguridad Taller V2 (002) RM. • DÍA_SEGURIDAD. Como resultado, se evidenció que además de la realización de la transferencia de conocimiento, se realizan refuerzo de los temas vistos.
A.7.2.3	Proceso disciplinario.	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Cumple parcialmente	De conformidad con el procedimiento "CID-C-01 Control Interno Disciplinario", se evidencia el procedimiento el cual se realiza la indagación de la queja en relación con el Código Único Disciplinario (Ley 734 de 2002) y el Estatuto Anticorrupción (Ley 1474 de 2011), **Sin embargo, en revisión contractual, no se estipula la Ley 1273 de Delitos Informáticos en Colombia.**
A.7.3 Terminación y cambio de empleo				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.7.3.1	Terminación o Cambio de responsabilidades de empleo.	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Cumple parcialmente	En revisión documental de los contratos en mención, se evidencia el numeral 28 "Seguridad de la Información", **sin embargo, no se identifica de forma clara y precisa en cuanto a la terminación o cambio de responsabilidades del empleo.**

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.8 – GESTIÓN DE ACTIVOS **A.8.1 – Responsabilidad por los activos**				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.8.1.1	Inventario de activos.	Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Cumple	Conforme con el formato GTI-F-05 Matriz de Inventario de Activos, Clasificación y Publicación de Información, se evidencia el diligenciamiento de los activos de información. Por otra parte, en la Guía de Inventario de Activos, Clasificación y Publicación de Información, se indica que la periodicidad de revisión se debe realizar en determinadas condiciones. Por lo tanto, **es importante considerar realizar una revisión periódica determinada independiente si no se presentan ningunas de las condiciones estipuladas.**
A.8.1.2	Propiedad de los activos.	Los activos mantenidos en el inventario deben tener un propietario.	Cumple	Conforme con el formato GTI-F-05 Matriz de Inventario de Activos, Clasificación y Publicación de Información, en el cual se tiene un total de 283 activos de información, todos con su respectiva asignación.
A.8.1.3	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.	Cumple	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política 6.4.1 Gestión de Activos, en la cual tiene identificada, clasificada, valorada y protegida la información conforme los intereses de la entidad.
A.8.1.4	Devolución de Activos.	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Cumple	De conformidad con el formato “GBS-G-01 Formato Entrega de Activos o Bienes Devolutivos – v3”, tiene como fin la devolución del bien activo, determinado en la caracterización del proceso de bienes y servicios. Adicional, se evidenció la política de borrado seguro, con el fin de evitar el traspaso de información no segura o reutilización de medios.
A.8.2 Clasificación de la información				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.8.2.1	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.	Cumple	Conforme con el formato GTI-F-05 Matriz de Inventario de Activos, Clasificación y Publicación de Información, se evidencia el diligenciamiento de los activos de información acorde al tipo de criticidad, requisitos legales.
A.8.2.3	Manejo de activos.	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema	Cumple	Conforme con los documentos GTI-F-05 Matriz de Inventario De Activos, Clasificación y Publicación de Información, GTI-G-01 Guía de Inventario de Activos, Clasificación y Publicación

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
		de clasificación de información adoptado por la organización.		De Información y por último Gtii-G-06 Guía de gestión de respaldo y restauración de copias de seguridad - v3. Se evidenció que tienen como objetivo brindar protección a la información en relación con: Almacenamiento, protección de copias, restricción de acceso de protección según los niveles de clasificación.
A.8.3 Manejo de medios				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.8.3.1	Gestión de medios removibles.	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Cumple parciamente	Conforme con el documento GTI-G-03 - GUÍA PARA LA MANIPULACIÓN DE MEDIOS Y BORRADO SEGURO, se expresa la tenencia del medio de almacenamiento en caso de renuncia, terminación o finalización del contrato. **Sin embargo, no se identifica que estos medios removibles cuenten con mecanismos criptográficos con el fin de garantizar la confidencialidad e integridad de la información.**
A.8.3.2	Disposición de los medios.	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Cumple	Conforme con el documento GTI-G-03 - GUÍA PARA LA MANIPULACIÓN DE MEDIOS Y BORRADO SEGURO, se expresa la tenencia del medio de almacenamiento en caso de renuncia, terminación o finalización del contrato. En el numeral 5.4 Borrado seguro, el profesional de soporte técnico se encarga de realizar el borrado seguro del medio de almacenamiento y deja registro de dicha actividad, adicional, se lleva un registro documental por parte del responsable del activo en donde autoriza la actividad a realizar.
A.8.3.3	Transferencia de medios físicos.	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Cumple	De conformidad con la política 6.4.15 Transferencia de Información, implementa controles para el aseguramiento de la información y evitar la pérdida de confidencialidad e integridad de la información empelando servicios de transporte o mensajería autorizada por la ANDJE.
A.9 – CONTROL DE ACCESO **A.9.1 – Requisitos del negocio para control de acceso**				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.9.1.1	Política de control de acceso.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Cumple	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política 6.4.2 Gestión de Acceso, en la cual se definen directrices para

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
				asegurar el acceso lógico y físico. Por consiguiente, esta Oficina evidenció que la Agencia cuenta con un sistema centralizado de directorio.
A.9.1.2	Acceso a redes y a servicios de red.	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Cumple	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política 6.4.2 Gestión de Acceso, se identifica que para los diferentes sistemas de información y servicios de red cuentan con requisitos de autenticación que debe ser otorgados con anterioridad con base en el procedimiento GTI-P-01 Procedimiento para Solicitud de Servicios de TI.
A.9.2 Gestión de acceso de usuarios				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.9.2.1	Registro y cancelación del registro de usuarios.	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Cumple	Conforme con el procedimiento GTI-P-01 Solicitud de Servicios de TI, todo supervisor o colaborador de la ANDJE deberá diligenciar el formato GTI-F-04 Solicitud de Servicios de Tecnología -V5, con el fin de realizar la creación, edición o eliminación de usuarios. Por lo tanto, esta Oficina evidenció que la OASTI remitió la circular interna 07 de 14 de julio de 2023 para todas las direcciones y oficinas de la ANDJE, indicando informar los cambios relacionados con ingreso, edición o retiro de personal. Como resultado, se constató que Secretaría General remitió a la OASTI el 15 de agosto el listado de 30 retiros.
A.9.2.2	Suministro de acceso de usuarios.	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Cumple	Conforme con el documento GTI-P-01 Procedimiento para Solicitud de Servicios de TI, todo supervisor o colaborador de la ANDJE deberá diligenciar el formato GTI-F-04 Solicitud de Servicios de Tecnología -V5, con el fin de realizar la creación, edición o eliminación de usuarios.
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Cumple	En revisión con el administrador del directorio activo, esta Oficina constató que el único usuario con derechos administrativos es el administrador del directorio activo.

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
				Members: Name / Active Directory Domain Services Folder Daniel Rojas ... ANDJE.LOCAL/DEFENSAJURIDICA/OFICINA ... Gilmar Lagos ... ANDJE.LOCAL/Deshabilitados Jorge Luis Lo... ANDJE.LOCAL/Deshabilitados Juan Carlos B... ANDJE.LOCAL/Deshabilitados Netvaultadmin ANDJE.LOCAL/USERADMIN
A.9.2.4	Gestión de información de autenticación secreta de usuarios.	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Cumple parcialmente	Conforme con el documento GTI-P-01 Procedimiento para Solicitud de Servicios de TI, todo supervisor o colaborador de la ANDJE deberá diligenciar el formato GTI-F-04 Solicitud de Servicios de Tecnología -V5; esta Oficina constató que la asignación de la clave si bien es de manera temporal, emplea un nivel bajo de seguridad en su fortalecimiento criptográfico.
A.9.2.5	Revisión de los derechos de acceso de usuarios.	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Cumple	Conforme con el documento GTI-P-01 Procedimiento para Solicitud de Servicios de TI, todo supervisor o colaborador de la ANDJE deberá diligenciar el formato GTI-F-04 Solicitud de Servicios de Tecnología -V5, con el fin de realizar la creación, edición o eliminación de usuarios. Por lo tanto, esta Oficina evidenció que la OASTI remitió la circular interna 07 de 14 de julio de 2023 para todas las direcciones y oficinas de la ANDJE, indicando informar los cambios relacionados con ingreso, edición o retiro de personal. Como resultado, se constató que Secretaría General remite el 15 de agosto el listado de 30 retiros.
A.9.2.6	Retiro o ajuste de los derechos de acceso.	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Cumple	
A.9.3 Responsabilidades de los usuarios.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.9.3.1	Uso de información de autenticación secreta.	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Cumple parcialmente	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política 6.4.2 Gestión de Acceso, se identifica que la OASTI se encarga de suministrar los permisos para los diferentes sistemas de información y la asignación de claves de los usuarios. **Sin embargo, no es posible identificar una política para el correcto manejo de contraseñas, en relación con: Largo, tiempo de vida, atributos, entre otras**. Por otra parte, a la fecha del presente informe la OASTI, está en implementación de una matriz de roles y responsabilidades con el fin de poder gestionar con mayor facilidad las obligaciones de cada colaborador al interior de la Agencia.
A.9.4 Control de acceso a sistemas y aplicaciones.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.9.4.1	Restricción de acceso a la información.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Cumple parcialmente	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política 6.4.2 Gestión de Acceso, se identifica que la OASTI se encarga de suministrar los permisos para los diferentes sistemas de información y la asignación de claves de los usuarios. **Sin embargo, no es posible identificar una política para el correcto manejo de contraseñas, en relación con: Largo, tiempo de vida, atributos, entre otras**. Por otra parte, a la fecha del presente informe la OASTI, está en implementación de una matriz de roles y responsabilidades con el fin de poder gestionar con mayor facilidad las obligaciones de cada colaborador al interior de la Agencia.
A.9.4.2	Procedimiento de ingreso seguro.	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Cumple parcialmente	De conformidad con lo expuesto en la política 6.4.2 Gestión de Acceso, **no fue posible identificar la finalización de sesiones inactivas después de un periodo de tiempo definido, tal cual como esta Oficina evidenció en aplicaciones como Orfeo y Daruma.**
A.9.4.3	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Cumple parcialmente	De conformidad con lo expuesto en el control 9.4.1 Uso de información de autenticación secreta, se reitera lo evidenciado.

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.9.4.4	Uso de programas utilitarios privilegiados.	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Cumple	De conformidad con lo evidenciado por esta Oficina, se tiene implementado una política de grupo en el directorio activo, la cual restringe a los usuarios la instalación de programas.
A.9.4.5	Control de acceso a códigos fuente de programas.	Se debe restringir el acceso a los códigos fuente de los programas	Cumple	De conformidad con la Guía para el Desarrollo de Software Seguro, tiene como objeto asegurar el software desarrollado o adquirido, cumpla con los requisitos de seguridad y calidad. Como lineamiento de verificación por parte de esta Oficina se evidenció ambientes de pruebas y producción para la aplicación Orfeo.
A.10 – CRIPTOGRAFÍA **A.10.1 – Controles Criptográficos**				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.10.1.1	Política sobre el uso de controles criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Cumple parcialmente	De conformidad con la política 6.4.16 Sobre el Uso de Controles y Llaves Criptográficas, esta Oficina reitera lo indicado en el control A.8.3.1 Gestión de medios removibles y 9.4.1 Uso de información de autenticación secreta.
A.10.1.2	Gestión de llaves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Cumple parcialmente	De conformidad con la política 6.4.16 Sobre el Uso de Controles y Llaves Criptográficas, no se identifica el tiempo de vida de las llaves criptográficas en los diferentes sistemas de información.
A.11 – SEGURIDAD FÍSICA Y DEL ENTORNO **A.11.1 – Áreas seguras**				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.11.1.1	Perímetro de seguridad física.	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	Cumple	De conformidad con la política 6.4.8 Seguridad Física y del Entorno, define las áreas seguras de la Agencia como el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia; deberán contar con mecanismos de protección física y ambiental, y controles de acceso físico para permitir únicamente los ingresos ajustados al cargo y funciones asignadas. Por consiguiente, esta Oficina evidenció en recorrido al Centro de Datos, que cuenta con medida de seguridad contra incendios y control de acceso físico.

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.11.1.2	Controles de accesos físicos.	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	Cumple	De conformidad con lo expuesto en el control A.11.1.1 Perímetro de seguridad física, esta Oficina evidenció la existencia de control biométrico al ingreso del Centro de Datos y el control de registro de todos los accesos mediante una bitácora. No obstante, se recomienda implementar un control biométrico gestionable el cual lleva registro de más exacto de los ingresos y salidas del Centro de Datos.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones.	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	Cumple	De conformidad con la política 6.4.8 Seguridad Física y del Entorno, esta Oficina reitera lo indicado en el control A.11.1.2 Controles de accesos físicos y A.11.1.1 Perímetro de seguridad física.
A.11.1.4	Protección contra amenazas externas y ambientales.	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Cumple	Con base en los documentos "GH-PN-06 PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS - V7" y el documento "Optimizar el Modelo de Gestión de Seguridad y Privacidad de la información y sistema de continuidad del negocio con base en lo definido en la norma técnica ISO27001, ISO 22301 y los lineamientos del gobierno nacional en materia de seguridad y privacidad de la información y Gobierno Digital", se diseña los planes contra los desastres naturales o accidentes.
A.11.1.5	Trabajo en áreas seguras.	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Cumple	De conformidad con la política 6.4.8 Seguridad Física y del Entorno, esta Oficina reitera lo indicado en el control A.11.1.2 Controles de accesos físicos y A.11.1.1 Perímetro de seguridad física.
A.11.1.6	Áreas de despacho y carga.	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Cumple	Protocolo Interno del Edificio.
A.11.2 Equipos				
ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.11.2.1	Ubicación y protección de los equipos.	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Cumple	De conformidad con la política 6.4.8 Seguridad Física y del Entorno y Protocolo Interno del Edificio.

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.11.2.2	Servicios de suministro.	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Cumple	Protocolo Interno del Edificio
A.11.2.3	Seguridad del cableado.	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Cumple	Protocolo Interno del Edificio
A.11.2.4	Mantenimiento de equipos.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Cumple	De conformidad con el contrato 133-2019 con UNIPAR ALQUILERES DE COMPUTADORES S.A. se indica que los computadores de la Agencia se encuentran en modalidad de arrendamiento, por tal motivo el mantenimiento de estos es ajeno al ANJDE. **Sin embargo, la OASTI realiza el mantenimiento preventivo por medio de una lista de chequeo, la cual consiste en verificación y corrección a nivel de software.**
A.11.2.5	Retiro de activos.	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	Cumple	Al respecto, se evidencia la existe de un formato [GTI-F-07] ACTA DE ENTREGA DE EQUIPOS DE CÓMPUTO - V1, el cual debe diligenciarse por parte del personal en el momento de retiro, desvinculación laboral. Por lo tanto, esta Oficina realizó un muestreo simple de tres actas de entrega de equipos de cómputo de los siguientes usuarios (ana.nieto, eliana.labrador, freddy.osorio), evidenciando la devolución del activo.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Cumple parcialmente	De conformidad con la política 6.4.16 Uso de Controles y Llaves Criptográficas, esta Oficina reitera lo indicado en el A.8.3.1 Gestión de medios removibles.
A.11.2.7	Disposición segura o reutilización de equipos.	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o re uso.	Cumple	De conformidad con el formato "GBS-G-01 Entrega de Activos o Bienes Devolutivos – v3", tiene como fin la devolución del bien activo, determinado en la caracterización del proceso de bienes y servicios. Adicional, se evidenció la política de borrado seguro, con el fin de evitar el traspaso de información no segura o reutilización de medios.

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.11.2.8	Equipos de usuario desatendido.	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Cumple	De conformidad con lo evidenciado por esta Oficina, se tiene implementado una política de grupo en el directorio activo, la cual bloquea las sesiones que tengan determinado tiempo de inactividad. **Sin embargo, conforme lo evidenciado se identificaron dos políticas así: Pantalla Bloqueo y Política Pantalla Bloqueo. Por lo tanto, esta Oficina recomienda realizar una depuración de las políticas de grupo con el fin de generar una adecuada administración.**
A.11.2.9	Política de escritorio limpio y pantalla limpia.	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Cumple	De conformidad con lo expuesto en el control A.11.2.8 Equipos de usuario desatendido, esta Oficina reitera lo evidenciado.
A.12 – SEGURIDAD DE LAS OPERACIONES **A.12.1 – Procedimientos operacionales y responsabilidades.**				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.12.1.1	Procedimientos de operación documentados.	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	Cumple	Documentación SIGI evidenciada en el aplicativo de Gestión Documental “Daruma”.
A.12.1.2	Gestión de cambios.	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Cumple	Conforme con el procedimiento [GTI-P-02] GESTIÓN DE CAMBIOS DE TI - V1, se recibe y se analizan los cambios solicitados por los usuarios e indica que se tiene que diligenciar el Formato GTI-F-010 SOLICITUD DE CAMBIOS. Por lo anterior, esta Oficina realizó la verificación documental de cuatro casos, constatando que se diligenció el formato en cuestión. 30274 – Aumento de memoria. 31265 – Aumento Disco C Servidor. 31642 – Aumento de memoria RAM Servidor. 32118 – Aumento memoria servidor.
A.12.1.3	Gestión de capacidad.	Se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los	Cumple parcialmente	Conforme con la guía GTI-G-07 GUÍA PARA LA GESTIÓN DE LA CAPACIDAD, se establece que por medio de la herramienta de Centreon se realiza el monitoreo de los

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
		requisitos de capacidad futura, para asegurar el desempeño requerido del sistema		servicios, exponiendo el estado actual de la infraestructura en relación con la capacidad. Adicional, se evidencia el documento Informe de Infraestructura el cual comprende un análisis de la infraestructura tecnológica durante los años 2022 y 2023, verificando la capacidad tecnológica y su desempeño. **Sin embargo, no se identifica con que periodicidad se toman los valores de referencia.**
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Cumple	De conformidad con la Guía para el Desarrollo de Software Seguro, tiene como objeto asegurar el software desarrollado o adquirido, cumpla con los requisitos de seguridad y calidad. Como lineamiento de verificación por parte de esta Oficina se evidenció ambientes de pruebas y producción para la aplicación Orfeo.
A.12.2 Protección contra códigos maliciosos.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.12.2.1	Controles contra códigos maliciosos.	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Cumple	De conformidad con la política 6.4.11 Protección contra código malicioso, implementa controles para evitar el uso de software no autorizado y la navegación en sitios web maliciosos mediante políticas de navegación en el firewall. Adicional, se realiza cada lunes se realiza una campaña de sensibilización que se llama “Lunes Seguro”.
A.12.3 Copias de respaldo.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.12.3.1	Respaldo de la información.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Cumple	De conformidad con la política 6.4.12 Copias de Respaldo y la guía GTI-G-06 Guía de gestión de respaldo y restauración de copias de seguridad - v3, esta Oficina evidenció que se realizan copias de seguridad conforme la periodicidad determinada, a su vez se realizan pruebas de certificación de las copias aleatoriamente.
A.12.4 Registro y seguimiento.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.12.4.1	Registro de eventos.	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario,	Cumple	Conforme con lo evidenciado en sesión en conjunto con la OASTI, en la actualidad la herramienta de monitoreo FortiSiem

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
		excepciones, fallas y eventos de seguridad de la información.		permite monitorear los eventos previamente parametrizados y así, se genere alertas sobre los posibles incidentes.
A.12.4.2	Protección de la información de registro.	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Cumple	
A.12.4.3	Registros del administrador y operador.	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Cumple	
A.12.4.4	Sincronización de relojes.	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Cumple	
A.12.5 Control de software operacional.				
ANEXO		**CONTROL**	**VALORACIÓN**	**OBSERVACION OCI**
A.12.5.1	Instalación de software en sistemas operativos.	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Cumple	De conformidad con lo expuesto en el control A.9.1.1 Política de control de acceso, esta Oficina reitera lo evidenciado.
A.12.6 Gestión de la vulnerabilidad técnica.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.12.6.1	Gestión de las vulnerabilidades técnicas.	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado	Cumple	Conforme con lo evidenciado en sesión en conjunto con la OASTI, en la actualidad la herramienta de monitoreo FortiSiem permite monitorear los eventos previamente parametrizados y así, se genere alertas sobre los posibles incidentes.
A.12.6.2	Restricción sobre la instalación de software.	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios	Cumple	De conformidad con lo expuesto en el control A.9.1.1 Política de control de acceso, esta Oficina reitera lo evidenciado.
A.12.7 Consideraciones sobre auditorías de sistemas de información				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.12.7.1	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Cumple parcialmente	Conforme con lo evidenciado en sesión en conjunto con la OASTI, si bien existen sistemas de información que se pueden parametrizar para que las auditorias tengan acceso a los logs de auditoría o a toda la información contenida bajo parámetros de lectura. Esto es posible en determinados sistemas, ya que esa opción no se encuentra implementada. Por ende, **se recomienda que todo sistema de información, presente y futuro puede ser parametrizado de tal forma que no afecte**

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
				el desempeño de la operación, apoyándose con la Matriz de Roles y Perfiles.
A.13 - SEGURIDAD DE LAS COMUNICACIONES **A.13.1 - Gestión de la seguridad de las redes**				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.13.1.1	Controles de redes.	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Cumple	De conformidad con la política 6.4.5 Uso de Internet, se establecen las reglas en el Firewall para el uso de internet seguro y por medio de Sistema de Monitoreo permite identificar las vulnerabilidades conforme lo expuesto en el control A.12.6.1 Gestión de las vulnerabilidades técnicas.
A.13.1.2	Seguridad de los servicios de red.	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	Cumple	
A.13.1.2	Separación en las redes.	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Cumple	Conforme con lo evidenciado en sesión en conjunto con la OASTI, esta Oficina identificó que se encuentran segmentados los diferentes activos, entre ellos: Redes inalámbricas, Servidores, Colaboradores.
A.13.2 Transferencia de información.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.13.2.1	Políticas y procedimientos de transferencia de información.	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	Cumple	De conformidad con el procedimiento GD-P-07 - TRANSFERENCIAS DOCUMENTALES PRIMARIAS - V4, se establecen los lineamientos para la transferencia de información al interior de la Agencia. Adicional, la política 6.4.15 Transferencia de Información, asegura la confidencialidad e integridad de la información.
A.13.2.2	Acuerdos sobre transferencia de información.	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	Cumple	De conformidad con lo expuesto en el control A.13.2.1 Políticas y procedimientos de transferencia de información, esta Oficina reitera lo evidenciado.
A.13.2.3	Mensajería electrónica.	Se debería proteger adecuadamente la información incluida en la mensajería electrónica	Cumple	De conformidad con la política 6.4.6 Uso de Comunicaciones Digitales, se identifican pautas para el buen manejo de comunicaciones como mensajería.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización parala protección de la información.	Cumple	De conformidad con la política 6.4.4 Seguridad para los Colaboradores, se evidencia la inclusión de la cláusula de confidencialidad "*Todos los colaboradores deben firmar un acuerdo de confidencialidad con la Agencia y se hacen responsables del cumplimiento de la debida diligencia para la*

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
				protección de la información que esté bajo su responsabilidad, reportando cualquier anomalía de acuerdo con la Política de Gestión de Incidentes de Seguridad de la Información"
A.14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS **A.14.1 - Requisitos de seguridad de los sistemas de información**				
ANEXO		**CONTROL**	**VALORACIÓN**	**OBSERVACION OCI**
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información.	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Cumple	De conformidad la documentación evidenciada, se cuenta con la Guía para el Desarrollo de Software Seguro, tiene como objeto asegurar el software desarrollado o adquirido, cumpla con los requisitos de seguridad y calidad; los procedimientos [GI-P-09] REALIZAR DESARROLLO Y PUESTA EN MARCHA DE LOS REQUERIMIENTOS EN EL SISTEMA UNICO DE INFORMACIÓN LITIGIOSA DEL ESTADO - V1 y [GTI-P-03] SOLICITUD Y APROBACIÓN DE NUEVOS DESARROLLOS O MEJORAS DE SOFTWARE - V2.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Cumple	De conformidad con la documentación evidenciada, se cuenta con procedimientos, políticas de cifrado de comunicaciones, sistemas de autenticación, sistema FortiSiem para la prevención y análisis de vulnerabilidades, finalmente la implementación de reglas de a nivel de firewall.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Cumple	De conformidad con la política 6.4.15 Uso de Comunicaciones Digitales, se identifican pautas para el buen manejo de comunicaciones como mensajería y la política 6.4.15 Transferencia de Información.
A.14.2 Seguridad en los procesos de desarrollo y de soporte.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.14.2.1	Política de desarrollo seguro.	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	Cumple	De conformidad con lo expuesto en el control A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación, se reitera lo evidenciado. Y el procedimiento GTI-P-02 Gestión de Cambios de TI el cual cumple con el propósito de analizar de forma controlada los cambios, a miras de minimizar traumatismos en la Agencia.
A.14.2.2	Procedimientos de control de cambios en sistemas.	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.		

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.		
A.14.2.4	Restricciones en los cambios a los paquetes de software.	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.		
A.14.2.5	Principios de construcción de los sistemas seguros.	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.		
A.14.2.6	Ambiente de desarrollo seguro.	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.		
A.14.2.7	Desarrollo contratado externamente.	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.		
A.14.2.8	Pruebas de seguridad de sistemas.	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.		
A.14.2.9	Prueba de aceptación de sistemas.	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.		
A.14.3 Datos de pruebas.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.14.3.1	Protección de datos de prueba.	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Cumple	De conformidad con lo expuesto en el control A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación, se reitera lo evidenciado. Y el procedimiento GTI-P-02 Gestión de Cambios de TI el cual cumple con el propósito de analizar de forma controlada los cambios, a miras de minimizar traumatismos en la Agencia.
A.16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN				

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.16.1 - Gestión de incidentes y mejoras en la seguridad de la información.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.16.1.1	Responsabilidades y procedimientos.	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Cumple	De conformidad con el procedimiento [GTI-P-05] GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION - V2, se tiene identificado los responsables de la gestión en cada uno de los pasos. Adicional, se tiene la conformación de un grupo de respuestas para los incidentes de seguridad.
A.16.1.2	Reporte de eventos de seguridad de la información.	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Cumple	De conformidad con el procedimiento [GTI-P-05] GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION - V2, se tienen identificados los canales para el reporte de incidentes de seguridad como: correo electrónico, dirección web (portal del sistema de gestión de servicios de tecnologías) y vía telefónica.
A.16.1.3	Reporte de debilidades de seguridad de la información.	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Cumple	De conformidad con el procedimiento [GTI-P-05] GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION - V2, se tienen identificados los canales para el reporte de incidentes de seguridad como: correo electrónico, dirección web (portal del sistema de gestión de servicios de tecnologías) y vía telefónica.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Cumple	De conformidad con el procedimiento [GTI-P-05] GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION - V2, se tiene identificado la verificación, aprobación, clasificación, criticidad, impacto y costo de los incidentes de seguridad de la información, el cual es valorador por el responsable de seguridad y privacidad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información.	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Cumple	De conformidad con el procedimiento [GTI-P-05] GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION - V2, se tiene identificado los responsables de la gestión en cada uno de los pasos. Adicional, se tiene la conformación de un grupo de respuestas para los incidentes de seguridad.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	Cumple	De conformidad con el procedimiento [GTI-P-05] GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION - V2, se tiene identificado el registro de la respuesta en la base de conocimiento.

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
A.16.1.7	Recolección de evidencia.	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Cumple	
A.17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO				
A.17.1 - Continuidad de seguridad de la información				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Cumple	De conformidad con el documento "Documento de pruebas, ejecución y resultados de DRP y BCP", esta Oficina evidenció la existencia de un plan de continuidad del negocio dirigido hacia los procesos críticos, documentación de pruebas, ejecución y resultados.
A.17.1.2	Implementación de la continuidad de la seguridad de la información.	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Cumple	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Cumple	
A.17.2 Redundancias.				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Cumple	Conforme con el documento "Informe de Infraestructura" y el contrato del centro de cómputo alterno con el proveedor IFX, constata la existencia de un centro de datos alterno para la ANDJE, el cual se encuentra contratado con IFX.
A.18 - CUMPLIMIENTO				
A.18.1 - Cumplimiento de requisitos legales y contractuales				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.18.1.1	Identificación de la legislación aplicable y de	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deben identificar y	Cumple	De conformidad con el documento "Normograma" se puede identificar los diferentes requisitos estatuarios pertinentes a la

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
	los requisitos contractuales.	documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.		seguridad de la información, entre ellos la Ley de 1581 de 2012 Protección de Datos Personales.
A.18.1.2	Derechos de propiedad intelectual.	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Cumple	De conformidad con la política 6.4.10 Desarrollo Seguro, tiene como medida el aseguramiento de que todo sistema de información o desarrollado cumpla con los acuerdos de licenciamiento en el cual se especifique las condiciones de uso y derechos de propiedad intelectual. Por lo tanto, como se manifiesta en el informe de Derechos de Autor del año 2022, no es posible la instalación de Software, manteniendo el control centralizado y así, el cumplimiento normativo vigente.
A.18.1.3	Protección de registros.	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Cumple	En el Manual de Políticas de Gestión y Desempeño Institucional de la Agencia, se encuentra definido la política de Gestión Documental, la cual se encuentra orientada a la gestión de la información física y electrónica, empleando la tabla de retención documental.
A.18.1.4	Privacidad y protección de información de datos personales.	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable	Cumple	De conformidad con la política 6.10 Tratamiento de la Información de Datos Personales, tiene como medida el aseguramiento de datos personales. Adicional, y como medida para el aseguramiento y cumplimiento en lo dispuesto en la política, esta Oficina evidenció que la OASTI realizó un seguimiento a todos los líderes de proceso para que informen si en sus procesos manejan bases de datos personales, con el fin de registrarlas ante la SIC.
A.18.1.5	Reglamentación de controles criptográficos.	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Cumple	De conformidad con la política 6.4.16 Sobre el Uso de Controles y Llaves Criptográficas, esta Oficina reitera lo indicado en el anexo A.10 – CRIPTOGRAFÍA.
A.18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN				
ANEXO		**CONTROL**	**VALORACIÓN**	**COMENTARIOS OCI**
A.18.2.1	Revisión independiente de la seguridad de la información.	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar	Cumple	Al respecto, se ha realizado una revisión anual al proceso y este es incluido dentro del Plan de auditorías de Control Interno de la ANDJE.

ANEXO		CONTROL	VALORACIÓN	COMENTARIOS OCI
		independientemente a intervalos planificados o cuando ocurran cambios significativos.		
A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	Cumple parcialmente	Al respecto, se recomienda fortalecer y medir el cumplimiento de las políticas y normas de seguridad.
A.18.2.3	Revisión del cumplimiento técnico.	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Cumple	De conformidad con la política 6.4.17 Uso Seguro de la Infraestructura Tecnológica, indica que la OASTI mantendrá monitoreará enlaces de red y componentes de software y se realizará análisis de vulnerabilidades. Adicional, el instructivo [GTI-I-03] INSTRUCTIVO PARA LA DISTRIBUCIÓN DE ACTUALIZACIONES - WSUS - V1 el cual busca centralizar las actualizaciones de los equipos de cómputo bajo sistemas operativos Windows.

– DIAGNOSTICO DEL PLAN DE CONTINUIDAD DEL NEGOCIO BCP Y PLAN DE RECUPERACIÓN DE DESASTRES DRP.

Tabla No. 4 Diagnostico Plan de Continuidad de Negocio y Plan Recuperación Desastres.

OBJETIVO	VALORACIÓN	COMENTARIOS OCI
Se establecen procedimientos específicos que respondan a las fallas o interrupciones del servicio.	Cumple	De conformidad con el documento BCP – Plan de Continuidad del Negocio sobre la estructura de la entidad, se tienen establecidos procedimientos específicos para los supuestos
Se tienen identificados los activos de información críticos para la operación del negocio.	Cumple	De conformidad con el documento BCP, se evidenciaron 15 procesos priorizados, los cuales se encuentran segmentados dada su criticidad así: 7 criticidad alta y el restante con criticidad media.
Se tienen identificados claramente las personas claves para la operación de las actividades claves del negocio	Cumple	De conformidad con el documento BCP, se tienen definidos los roles y responsabilidades del BCP los cuales se conforman en tres grupos estratégicos **ESTRATÉGICO** | **TÁCTICO** | **OPERATIVO** Adicional, se evidencia la conformación de equipos de recuperación de procesos críticos y equipos de recuperación tecnológica, con su respectivo responsable.
Se tiene definido un árbol de comunicación para la activación del BCP	Cumple	De conformidad con el documento BCP, se evidencia la conformación de un árbol de comunicación el cual se encuentra alineado con los niveles definidos por la Agencia.
Se tienen establecidos los tiempos mínimos para la recuperación - RTO	Cumple	De conformidad con el documento BCP y conforme con el nivel de criticidad de los procesos, se evidencia un RTO.
Se tienen establecidos los tiempos objetivos para la recuperación – MTPD	Cumple	De conformidad con el documento BCP y conforme con el nivel de criticidad de los procesos, se evidencia un MTPD.
Se tienen establecidos los tiempos objetivos para punto de recuperación – RPO	Cumple	De conformidad con el documento BCP y conforme con el nivel de criticidad de los procesos, se evidencia un MTPD.
Se tienen definidos los sistemas de información mínimos necesarios para la operación en caso de contingencia	Cumple	De conformidad con el documento Análisis de Impacto al Negocio, se identifica el Anexo 1 - P2E6 Documento con la identificación de impactos por cada proceso y los recursos mínimos.
Se tienen definidos los riesgos presentes para la continuidad	Cumple	De conformidad con el documento BCP, se tienen identificados según su factor de riesgo: **Entorno**: Sismo/Terremoto; Inundación; Tormenta eléctrica; Incendio/ explosión; Robo; Terrorismo; Bloqueos/Huelgas; Vecinos o establecimientos adyacentes de alto riesgo **Recurso Humano**: Suspensión de actividades por inconformidad de funcionarios; Pérdida de personal clave; Epidemia / Pandemia; Intoxicación – Infección Alimentaria; Accidente Masivo; Secuestro **Infraestructura Tecnológica**: Falla de las aplicaciones / servicios de TI; Pérdida de información; Incidentes de seguridad de la información; Fallas de los proveedores de TI **Proveedores**: Ausencia de proveedores críticos para la operación
Se tienen procedimientos desarrollados o guías de operación en caso de desastre para cada uno de los servicios críticos	Cumple	De conformidad con el documento BCP, se tienen definido las actividades siguientes: Plan de activación y recuperación, Plan de Contingencia y Retorno de Operación Normal. Cada actividad está diseñada para los escenarios identificados.
Se realiza capacitaciones que tengan como finalidad garantizar el correcto funcionamiento del plan	Cumple	De conformidad con el documento BCP, se planteó el supuesto: "*Los grupos de trabajo integrantes de los equipos de recuperación de procesos y tecnologías han sido capacitados y entrenados oportunamente*". Por lo tanto, esta Oficina en verificación documental, evidenció el Documento de pruebas,

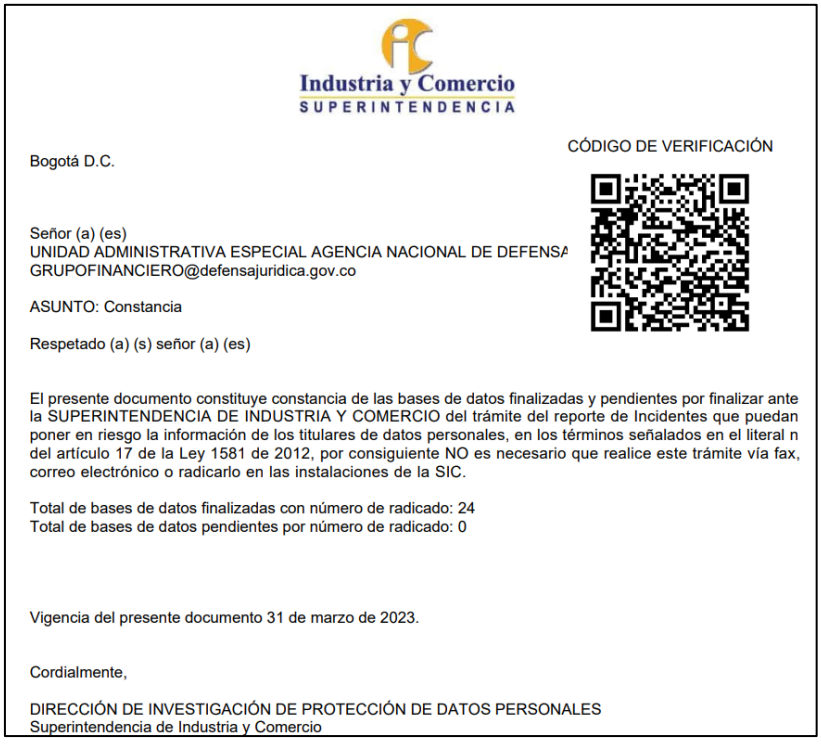
OBJETIVO	VALORACIÓN	COMENTARIOS OCI
		ejecución y resultados de DRP y BCP, en el cual se realizó un entrenamiento con los diferentes escenarios.
Se establecen planes de pruebas, gestión y mantenimientos con el fin de garantizar los objetivos del plan	Cumple	Conforme con el documento "P3E37: Documento de pruebas, ejecución y resultados de DRP y BCP", se evidencia que el 02 de agosto de 2022 se realizó una prueba de conocimiento de los diferentes actores que se involucran en el BCP. Por otra parte, el BCP tiene como fecha de publicación agosto de 2022 y se ha determinado que se debe realizar una prueba al año, a la fecha de emisión del presente informe no se ha realizado.

- IDENTIFICACIÓN BASES DE DATOS PERSONALES

En el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), la OASTI realizó un levantamiento de información con los líderes de los procesos sobre las bases de datos con datos personales y de las cuales reposen en sus repositorios institucionales y como resulto se obtuvo un total de 22 bases de datos entre todos los líderes de la ANDJE.

Así las cosas, esta Oficina solicito a la OASTI la evidencia del registro de las bases datos ante Superintendencia de Industria y Comercio (SIC), obteniendo que la ANDJE registro ante la SIC un total de 24 bases de datos conforme la siguiente imagen:

Imagen No. 1 Registro de la ANDJE ante el SIC



Industria y Comercio
SUPERINTENDENCIA

CÓDIGO DE VERIFICACIÓN

Bogotá D.C.

Señor (a) (es)
UNIDAD ADMINISTRATIVA ESPECIAL AGENCIA NACIONAL DE DEFENSA
GRUPOFINANCIERO@defensajuridica.gov.co

ASUNTO: Constancia

Respetado (a) (s) señor (a) (es)

El presente documento constituye constancia de las bases de datos finalizadas y pendientes por finalizar ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite del reporte de Incidentes que puedan poner en riesgo la información de los titulares de datos personales, en los términos señalados en el literal n del artículo 17 de la Ley 1581 de 2012, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

Total de bases de datos finalizadas con número de radicado: 24
Total de bases de datos pendientes por número de radicado: 0

Vigencia del presente documento 31 de marzo de 2023.

Cordialmente,

DIRECCIÓN DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES
Superintendencia de Industria y Comercio

3. Conclusiones:

En concordancia con la Norma ISO 27001 y el Instrumento de Evaluación del MSPI, en el cual la Oficina de Control Interno realizó la verificación de 100 controles, con el fin de poder validar su cumplimiento normativo. Así las cosas, se constató que el 84% de los controles auditados presentan un estado de validación como CUMPLIDO y el restante 16% como CUMPLE PARCIALMENTE.

4. Recomendaciones

Conforme los dominios de la Norma ISO 27001:2013, la Oficina de Control Interno recomienda:

DOMINIO	RECOMENDACIÓN OCI
Dominio 5 - Política de Seguridad de la Información	• No se tienen recomendaciones por parte del OCI
Dominio 6 - Organización de la seguridad de la información	• Generar un procedimiento sobre la segregación de responsabilidades.
Dominio 7 - Seguridad de los Recursos Humanos	• Inclusión contractual de la Ley 1273 del 2009 Protección de la información y de los datos. • Precisar de forma más clara las responsabilidades y deberes en relación con la terminación o cambio de responsabilidades del empleo, con respecto al numeral 28 “Seguridad de la Información”.
Dominio 8 - Gestión de activos	• Implementar mecanismos criptográficos a los medios removibles, con el fin de garantizar la confidencialidad e integridad de la información.
Dominio 9 - Control de acceso	• Fortalecer los mecanismos de gestión de información de autenticación secreta de usuarios. • Implementar una Matriz de Roles y Responsabilidades • Fortalecer los mecanismos de bloqueo de sesiones inactivas para los diferentes sistemas de información.
Dominio 10 - Criptografía	• Tener un registro documental de los poseedores de las llaves criptográficas y su tiempo de vida durante todo el ciclo.
Dominio 11 - Seguridad física y del entorno	• No se tienen recomendaciones por parte del OCI
Dominio 12 - Seguridad de las operaciones	• Precisar la periodicidad con que se realiza la verificación de la capacidad tecnológica. • Fortalecer la capacidad de gestión en los sistemas de información, sobre la parametrización de perfiles de auditoría.
Dominio 13 - Seguridad de las comunicaciones	• No se tienen recomendaciones por parte del OCI
Dominio 14 - Adquisición, desarrollo y mantenimiento de sistemas	• No se tienen recomendaciones por parte del OCI
Dominio 16 - Gestión de incidentes de seguridad de la información	• No se tienen recomendaciones por parte del OCI
Dominio 17 - Aspectos de seguridad de la información de la gestión de continuidad de negocio	• No se tienen recomendaciones por parte del OCI
Dominio 18 - Cumplimiento	• Fortalecer y medir el cumplimiento de las políticas y normas de seguridad

Vale la pena mencionar que previo a la emisión del presente informe final, el Líder del proceso de Gestión de Tecnologías de la Información remitió a esta Oficina, un correo electrónico el 12 de septiembre del año en curso con algunas observaciones mediante el cual dieron respuesta al Informe Preliminar, las cuales fueron tenidas en cuenta en lo pertinente para la emisión del presente Informe Final.

Respuesta del proceso TIC: Una vez revisado el informe preliminar se presentan las siguientes observaciones:

En el Dominio 6 - Organización de la seguridad de la información.
Recomendación: Generar un procedimiento sobre la segregación de responsabilidades
Respuesta OASTI: Considero que se debe indicar que se debe realizar un lineamiento y no un procedimiento.

En el Dominio 9 - Control de acceso

Recomendación: Fortalecer los mecanismos de gestión de información de autenticación secreta de usuarios.
Fortalecer los mecanismos de bloqueo de sesiones inactivas para los diferentes sistemas de información.

Comentario Oficina de Control Interno: A continuación, esta Oficina se permite responder las observaciones generadas:

En el Dominio 6 - Organización de la seguridad de la información.
De conformidad con lo manifestado por el proceso TIC, acoge la observación en la realización de un lineamiento.

En el Dominio 9 - Control de acceso:

a. En conformidad con lo evidenciado por esta Oficina, las contraseñas remitidas por parte de la OASTI en el inicio contractual con la ANDJE, se constató que estás carecen de mecanismos de cifrado fuerte, ya resultan fáciles de adivinar (año y lugar de trabajo). Adicional, no se identificó solicitud de cambio obligatorio de contraseña al momento de iniciar por primera vez.
b. En conformidad con lo evidenciado por esta Oficina, se constató que los sistemas de información Orfeo y Daruma, permiten permanecer estar conectados durante largos periodos de tiempo de inactividad. Por lo tanto, es importante que la sesión se bloquee después de un periodo de tiempo de inactividad y se solicite las credenciales nuevamente para ingresar al sistema.

Así las cosas, esta Oficina reitera la recomendación del presente informe.

Para constancia se firma en Bogotá D.C., a los 14 días del mes de septiembre del año 2023

Jefe de la Oficina de Control Interno (E.)
Nota. Los anexos al presente informe hacen parte integral.

Anexo No. 1 (si se requiere)
Informe de Auditoría al Plan de Seguridad y Privacidad de la Información

Especificaciones de la auditoria Informes de ley o Seguimiento:

- **Criterios:**
  - Ley 1581 de 2012. disposiciones generales para la protección de datos personales.
  - Ley 1712 de 2014. Ley de Transparencia.
  - Ley 1955 de 2019 Plan nacional de desarrollo 2018-2022 – Art.147 Transformación digital Art. 148 Gobierno digital como política de gestión.
  - Decreto 1244 de 8 de octubre de 2021 creación de la Oficina Asesora de Sistemas y Tecnologías de la información en la Agencia
  - Decreto 1008 de 2018, el cual modificó el Decreto 1078 de 2015, en su artículo 2.2.9.1.1.3 definió la seguridad de la información como principio de la Política de Gobierno Digital.
  - Decreto 1244 de 8 de octubre de 2021 creación de la Oficina Asesora de Sistemas y Tecnologías de la información en la Agencia.
  - Manual de Gobierno Digital - MinTic
  - Guía para la administración del riesgo y el diseño de controles en entidad públicas
  - Modelo de Seguridad y Privacidad de la Información - MinTic
  - NTC ISO/IEC 27001
  - Demás normatividad interna y externa aplicable

- **Plan de muestreo:**

La muestra se determinó mediante muestreo aleatorio simple, en donde se verificó la información:

TIPO DE INFORMACION	IDENTIFICADORES
Actas de Entrega de Equipos de Cómputo	ana.nieto – eliana.labrador – freddy.osorio
Capacitaciones	Charla Seguridad _Practicas seguras trabajo en casa Charla Seguridad de la Información _ Higiene Digital Charla Seguridad de la Información _Riesgos en el Mundo Virtual Cyberseguridad Taller V2 (002) RM DÍA_SEGURIDAD
Contratos por Prestación de Servicios de Apoyo a la Gestión	001 – 055 y 084 de 2023
Formatos de Inscripción a Teletrabajo	29969 – 29103 – 29102 – 28741
Formato de Solicitud de Cambios	30274 – 31265 – 31642 – 32118

- **Documentos Examinados:**
  - Documentos asociados al proceso

- **Carpetas compartidas**
  - AGOSTO_SGSI - OneDrive