FECHA DE EMISIÓN DEL INFORME	Día:	09	Mes:	Octubre	Año:	2025

Aspecto Evaluable (Unidad Auditable):	**MSPI - Modelo de Seguridad y Privacidad de la Información**
Líder de Proceso / Jefe(s) Dependencia(s):	Carlos Andrés Ballesteros Castañeda Subgerente de Tecnologías de Información y Comunicaciones
Objetivo de la Auditoría:	1. Evaluar la gestión de tecnologías de la información en la entidad, con énfasis en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de Identificar su estado actual, así como riesgos, brechas y oportunidades de mejora. 2. Identificar variaciones en los procesos frente a la documentación de estos. 3. Definir y acordar planes de acción que permitan el mejoramiento de los procesos. 4. Verificar los riesgos y controles establecidos dentro de los procedimientos.
Alcance de la Auditoría:	El alcance de la auditoría estará comprendido entre el 30 de junio del 2024 al 30 de mayo del 2025 y se desarrollará entre el 13 de junio al 30 de septiembre 2025, y estará enfocado al MSPI - Modelo de Seguridad y Privacidad de la Información, alineado con los dominios establecidos en la norma NTC-ISO/IEC 27001: 2013 y 2022.
Criterios de la Auditoría:	1. Documento Maestro Modelo de Seguridad y Privacidad de la Información 2. Herramienta de Diagnostico de Seguridad y Privacidad de la Información, de MINTIC. 3. Norma técnica Colombiana NTC-ISO-IEC 27001:2013 y 2022

ASPECTOS GENERALES

Teniendo en cuenta que, a la fecha del inicio de la auditoría, el Modelo de Seguridad y Privacidad de la Información – MSPI, previsto en el Anexo 1 de la Resolución 500 de 2021, estaba soportado en la norma ISO 27001 versión 2013, y que posteriormente se emitió Resolución 02277 del 3 de junio 2025, en la que se actualiza la referencia de la norma ISO 27001 por la versión 2022“, esta auditoría utilizará ambas versiones, considerando que el Modelo aplicado por la entidad ya estaba ajustado a la versión 2022.

Para realizar la auditoría de Gestión de TI, se utilizó la clasificación de los dominios establecidos en la norma NTC: ISO/IEC 27001:2013.

1. Políticas de seguridad de la información
2. Organización de la seguridad de la información
3. Gestión de activos
4. Control de acceso
5. Criptografía

6. Seguridad física y del entorno
7. Seguridad de las operaciones
8. Seguridad de las comunicaciones
9. Adquisición, desarrollo y mantenimientos de sistemas
10. Relación con los proveedores
11. Gestión de incidentes de seguridad de la información
12. Gestión de continuidad de negocio
13. Cumplimiento

Lo anterior, soportado en los siguientes procedimientos y Políticas de la Gestión de Tecnología de la Información y Comunicación:

- Política de Seguridad y Privacidad de la Información
- Manual de Políticas de Seguridad de la Información
- Política Tratamiento de Datos
- Gestión de Acceso a Servicios Tecnológicos
- Procedimiento Gestión y Soporte Servicios TIC
- Procedimiento Gestión Activos Información
- Procedimiento Gestión Incidentes Seguridad
- Procedimiento Gestión Vulnerabilidades
- Desarrollo y Mantenimiento de Sistemas de Información

NORMATIVIDAD ASOCIADA

- Resolución 500 del 10 de marzo de 2021 de MINTIC “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”.

- Resolución 2277 del 03 de junio del 2025 de MINTIC “Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”.

- Ley 1581 de 2012 Protección de Datos Personales

- Ley 1712 de 2014: Transparencia y Acceso a la Información Pública

- NTC-ISO-IEC 27001:2013 y 2022

- Guía para la Gestión y Clasificación de Activos de Información (MINTIC)

- NTC ISO/IEC 22301:2019: Sistema de gestión de continuidad de negocio.

ACTIVIDADES DESARROLLADAS

Para el desarrollo de la auditoría se validó para cada dominio de la Norma 27001:2013, las políticas, procedimientos y documentación soporte suministrada por la Subgerencia de Tecnologías de Información y Comunicaciones, verificando:

a. La trazabilidad documental requerida en cada control, así:

1. Políticas de seguridad de la información
   - Matriz de Aplicabilidad ATENEA 2025
   - PO1_TIC Política de Seguridad y Privacidad de la Información V2
   - Resolución 294 de Noviembre 2024 PO1_TIC V2.
   - Acta 14 Comité G D 02072024
   - Comité G&D 02072024
   - Publicación de la Política

2. Organización de la seguridad de la información
   - Responsables de la gestión de la seguridad de la información.
     - Estructura_Interna_SubTICS_2025
     - Organización interna SubTIC
   - Funciones de seguridad y privacidad de la información
     - Acuerdo 003_2021 ATENEA - Consejo Directivo
     - Res. DG-030 Manual Funciones ATENEA 2025
     - Resolución No 30 Comité Institucional de Gestión y Desempeño_0
   - Presupuesto asignado a las actividades del MSPI
     - PAA_2024 / PAA_2025
   - Plan de capacitación, sensibilización y comunicación de seguridad de la información
     - 2024 / Cultura y Apropiación
     - 2024 / Cultura y Apropiación / Piezas graficas
     - 2024 / Cultura y Apropiación / Sesiones
     - 2024 / Cultura y Apropiación / Simulación Directivos
     - 2024 / Cultura y Apropiación / Simulación Usuarios
     - 2024 / Cultura y Apropiación / Cultura y Apropiación Seguridad 2024
     - 2025 / Cultura y Apropiación / Cultura y Apropiación Seguridad 2025
     - 2025 / Cultura y Apropiación / Piezas graficas
     - 2025 / Entornos Digitales Seguros ATENEA
     - 2025 / Memorando PIC Seguridad 2025
   - Matriz de riesgos - Gestión Seguridad de la Información
     - 2024 / Riesgos_Seguridad_Administrativa_2024
     - 2024 / Riesgos_Seguridad_CID_2024
     - 2024 / Riesgos_Seguridad_Estrategia_2024
     - 2024 / Riesgos_seguridad_Posmedia_2024
     - 2024 / Riesgos_Seguridad_TICS_2024

- 2025 / Riesgos_Seguridad_CID_2025
- 2025 / Riesgos_Seguridad_Administrativa_2025
- 2025 / Riesgos_seguridad_Estrategica_2025
- 2025 / Riesgos_Seguridad_TICS_2025

- Comité sobre la política de Seguridad de la Información, los riesgos o incidentes de Seguridad de la Información
  - Acta 18 Comité G & D 19122024
  - Acta 19 31012025 (Firmas)
  - Acta 20 G&D 26022025 Firmada
- Soportes socialización o sensibilización de la Política de Seguridad de la Información
  - Conoce tus responsabilidades en la Seguridad de la Información
  - Programación Capacitación equipo BPO
- Soporte de inscripción a membrecías de grupos o foros de interés especial en seguridad de la información
  - Contacto_OEA
  - Contacto_OEA2
  - Contacto_OEA3
  - Grupo_Seguridad_Distrital
  - Lanic_04.07.2024
  - Lanic_30.09.2024
- Boletines emitidos por COLCERT sobre vulnerabilidades emergentes, amenazas activas.
  - Alerta de seguridad - Análisis de vulnerabilidad que afecta navegadores web
  - Boletín - Oracle lanza actualización de 378 parches de seguridad.msg
  - Vulnerabilidades FORTINET.msg
- Soporte de las obligaciones del contrato que asume rol del Oficial de Seguridad:

a. Realizar y hacer seguimiento al estado de la seguridad de la información y la privacidad en la Agencia ATENEA, identificando brechas, vulnerabilidades y riesgos asociados, en alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI).
   - Abril / Obligación_1 / Criterios de accesibilidad SICORE
   - Abril / Obligación_1 / FURAG Gobierno Digital
   - Abril / Obligación_1 / Opciones pendientes FURAG
   - Abril / Obligación_1 / Plan análisis vulnerabilidades servicio en nube
   - Abril / Obligación_1 / Preguntas gobierno digital
   - Abril / Obligación_1 / Solicitud de aclaración respecto a la pregunta del FURAG
   - Mayo / Obligación_1 / Boletín Chihuahua Infosteale
   - Mayo / Obligación_1 / Boletín de Alerta – Actividad del Ransomware Lynx
   - Mayo / Obligación_1 / DarkTrace_Infraestructura
   - Mayo / Obligación_1 / Implementación Darktrace
   - Mayo / Obligación_1 / Reporte Gestión de Riesgo corte 1
   - Mayo / Obligación_1 / Seguimiento_Darktrace_06052025

- Mayo / Obligación_1 / Vulnerabilidades FORTINET

b. Identificar implementar y hacer seguimiento a los controles específicos de seguridad y privacidad recomendados por el MSPI, garantizando su adecuación a los procesos y sistemas tecnológicos de la Agencia.
   - Abril / Obligación_2 / Diligenciamiento Matriz de roles y perfiles
   - Mayo / Obligación_2 / Diligenciamiento Matriz de roles y perfiles
   - Mayo / Obligación_2 / Doble factor de autenticación VPN
   - Mayo / Obligación_2 / Memorandos de solicitud
   - Mayo / Obligación_2 / Primer_Seguimiento
   - Mayo / Obligación_2 / Solicitud informacion correo modulo agendamiento
   - Mayo / Obligación_2 / Solicitud_Actualizacion_Esquema

c. Revisar, actualizar y desarrollar políticas, procedimientos y manuales relacionados con la seguridad de la información y privacidad, en cumplimiento con normativas locales e internacionales, incluyendo las leyes aplicables en Colombia
   - Abril / Obligación_3 / Actualización Manual de Politicas de Seguridad
   - Abril / Obligación_3 / Check list disgnostico AE en TI
   - Abril / Obligación_3 / Checklist dominios AE para Diagnóstico 2025 TI
   - Abril / Obligación_3 / Manual de Politicas de Seguridad de la Información 2025
   - Mayo / Obligación_3 / Datos Personales Requerimiento STIC
   - Mayo / Obligación_3 / Política para el Tratamiento de Datos Personales
   - Mayo / Obligación_3 / UTF-8Politica Tratamiento Datos Personales IA [REV HAP]

d. Definir y documentar protocolos para la identificación, análisis, respuesta y recuperación ante incidentes de seguridad, asegurando la continuidad operativa y mitigando posibles impactos.
   - Abril / Obligación_5 / Actualización sobre el Ransomware VanHelSing
   - Abril / Obligación_5 / Alerta de seguridad -Análisis de vulnerabilidad que afecta navegadores web.
   - Abril / Obligación_5 / Boletín - Oracle
   - Abril / Obligación_5 / Vulnerabilidad CVE-2025-3066 en Google Chrome
   - Mayo / Obligación_5 / Procedimiento copias de seguridad
   - Mayo / Obligación_5 / Procedimiento_Copias_Seguridad_2025
   - Mayo / Obligación_5 / Revisión procedimiento copias de seguridad

3. Gestión de activos
   - Activos de información ATENEA 2024
   - Acta 20 G&D 26022025 Firmada

4. Control de acceso
   - Relación de usuarios y roles del sistema
     - Kactus / A.Listado usuarios kactus
     - Kactus / B.Roles y accesos Kactus
     - Seven / A.Listado Usuarios Seven
     - Seven / B.Roles y accesos SEVEN
     - SICORE / A.Usuarios del sistema
     - SICORE / B.Roles y accesos

   - Revisión realizada sobre los usuarios activos 2do semestre 2024 y 1er semestre 2025.
     - Correo_17.03.2025
     - Formato (16.06.2025) (1) (1)
     - Novedades sobre funcionarios y cumplimiento del procedimiento
     - RE_ Solicitud contratistas y funcionarios ATENEA

   - Revisión efectuada sobre los accesos con privilegios del 1er semestre 2025.
     - Actualizacion_roles_Perfiles
     - Roles_Perfiles_RACI_ATENEA

   - Generalidades gestión acceso
     - Descripción_Sistemas
     - Administracion_Centralizada (Azure Active Directory)

   - Redes Servicios, Monitoreo tráfico
     - Redes_Servicios
     - Medios_Usados
     - Usuarios_VPN
     - Darktrace_mayo_2025
     - Reporte mayo 2025 - INTERNEXA
     - INFORME DE GESTIÓN AGENCIA ATENEA ABRIL 2025
     - INFORME DE GESTIÓN AGENCIA ATENEA MAYO 2025

   - Soporte de la solicitud de creación usuarios de SICORE – Contraseña, parámetros:
     - latuesta@agenciaatenea.gov.co.msg
     - mcifuentes@agenciaatenea.gov.co.msg
     - permanenciaupn_atenea@upn.edu.co
     - sestupinan@agenciaatenea.gov.co
     - Evidencia_Contraseña_SICORE
     - Recuperar_Contraseña

5. Seguridad de las operaciones
   - Procedimientos de operación de la Gestión de TIC documentados y formalizados.
     - P1_TIC: Procedimiento de Gestión de Activos de Información
     - P2_TIC: Procedimiento de Gestión de Incidentes de Seguridad

- P3_TIC: Procedimiento de Gestión de Vulnerabilidades
- P4_TIC: Procedimiento de Gestión de Acceso a Servicios Tecnológicos
- P5_TIC: Procedimiento de Desarrollo y Mantenimiento de Sistemas de Información
- P6_TIC: Procedimiento de Gestión y Soporte de Servicios TIC
- P7_TIC: Procedimiento de Gestión de Cambios en Infraestructura Tecnológica

- Gestión de copias de respaldo y recuperación de datos e información
  - Evidencia_Politica_Backups
  - G4_TIC Guía Institucional de Copias de Seguridad V1
  - Evidencia_Backups_SICORE
  - Certificacion de Seguridad - Atenea - Backups 2025 (DigitalWare)
  - Acta_DRP_SIGA_2025_Firmado-1
  - Evidendias ejecución DRP SIGA 2025

- Uso de recursos, así como proyecciones de los requisitos de capacidad futura
  - Gestión eventos-monitoreo SICORE
  - Proyección_Creditos_Nube

- Vulnerabilidades y plan de remediación
  - 2024 / Análisis_SIGA
  - 2024 / Remediación_SIGA
  - 2025 / Análisis_Academia_Atenea_Landing
  - 2025 / Análisis_Academia_Atenea_LMS

- Revisión sobre las actividades de los usuarios, sistema SICORE.
  - Solicitud creacion usuarios y contraseñas ies (je3 pt1)
  - Solicitud creacion usuarios y contraseñas instituciones etdh
  - Validación Piloto JE2

- Actividades del administrador y del operador del sistema SICORE
  - Soporte_Actividades_Administrador_SICORE
  - Roles_Politica
  - Servidores_SICORE
  - Respuesta_Seven_Kactus

6. Adquisición, desarrollo y mantenimientos de sistemas
   - Historias de usuarios - criterios de aceptación
     - HU SICORE 2025 / 20250219_TCF3_AjustesInscripcion
     - HU SICORE 2025 / 20250508_HU01_ConsultaApoyoEspecieTransmilenio
     - HU SICORE 2025 / 20250513_HU01_LiquidacionPagoIES_ Parametrizar Liquidación _(Pago 2)
     - HU SICORE 2025 / 20250513_HU02_LiquidacionPagoIES_Liquidación_(Pago 2)

- HU SICORE 2025 / 20250513_HU03_LiquidacionPagoIES_FlujoAprobación (Pago 2)
- HU SICORE 2025 / 20250513_HU04_LiquidacionPagoIES_SolicitudDocumentos (Pago 2)
- HU SICORE 2025 / 20250521_HU01_Renovación_ReporteIES_(Pago 2)_V2
- HU SICORE 2025 / 20250521_HU02_Renovación_ValidaciónPosmedia_(Pago 2)_V2
- HU SICORE 2025 / 20250521_HU03_Renovación_FlujoAprobaciónPosmediaIES (Pago 2)_V2
- HU SICORE 2025 / 20250804_HU01_Renovación_Matriculados (Pago 1 y 2)

- Casos de Prueba de los desarrollos
  - 20250211_Pruebas_Formalización_ReporteIES
  - 20250217_Pruebas_CreacionConvocatoriasConvenios (POSMEDIA)

7. Gestión de incidentes de seguridad de la información
   - Incidentes y Eventos Seguridad 2024 / 2025
   - Certificación NO incidentes 2025
   - Certificación NO incidentes 20243-2024-6587_1

8. Gestión de continuidad de negocio
   - PL4_TIC Plan de Recuperación Ante Desastres DRP V1
   - Acta_DRP_portalweb_2024
   - Prueba de recuperación a travérs del DRP servicios críticos
   - Acta_Estrategia_DRP
   - Acta_Socialización_DRP
   - Plan_DRP_2024_2025

b. Cruce de archivos Usuario, Roles, Funcionarios, Contratistas, Retirados y Ausentismo, para los sistemas de Información:
   - SICORE
   - KACTUS
   - SEVEN

c. Prueba de recorrido a los procesos de Gestión de Accesos para el sistema SICORE, validando:
   - Configuración de parámetros de contraseñas
   - Autenticación
   - Administración de accesos (Creación, modificación, desactivación y eliminación)
   - Asignación de roles y perfiles
   - Custodia de la clave del usuario administrador
   - Logs de Auditoría

Como resultado de la auditoría, la Oficina de Control Interno de Gestión, identificaron los siguientes hallazgos:

No.	HALLAZGOS	RECOMENDACIÓN	PLAN DE ACCIÓN
1.	**Responsabilidades Y Organización Seguridad Información**		
1.1	**Rol de Oficial de Seguridad de la Información** Criterio: **La Resolución 500 de 2021, de MINTIC establece en el numeral 7.2.3 "Roles y responsabilidades":** *"… Se debe delegar a una persona responsable de la seguridad y privacidad de la información, así como conformar el equipo humano necesario para coordinar la implementación del MSPI. Si este cargo no existe en la entidad, deberá designarse mediante acto administrativo y depender de un área estratégica diferente de la Oficina o Dirección de Tecnología (preferentemente del despacho del nominador). Asimismo, la persona designada debe ser incluida como miembro del comité de gestión institucional con voz y voto, y en el comité de control interno con voz."* El rol de Oficial de Seguridad de la Información no está definido dentro de la estructura orgánica de la Agencia, las funciones de seguridad de la información están a cargo de la Subgerencia TIC, las cuales se apoyan mediante la ejecución de un contrato de prestación de servicios que incluye obligaciones asociadas al rol. Esta situación limita su independencia, autoridad y visibilidad estratégica dentro de la entidad, y además lo expone a potenciales conflictos de interés, especialmente si el mismo equipo que implementa los sistemas es responsable también de monitorear el cumplimiento del Modelo.	El MSPI requiere un enfoque colaborativo entre distintas áreas de la entidad, por lo cual se recomienda validar la adopción de las siguientes acciones para alinear la estructura organizacional con las mejores prácticas y los lineamientos de la Resolución 500 de 2021: a. Redefinir la dependencia jerárquica del Oficial de Seguridad de la Información, para que esta posición reporte directamente a la Alta Dirección o al Comité de Riesgos de la entidad. Esto asegurará su autonomía, evitará conflictos de interés y permitirá que las decisiones en materia de seguridad de la información se tomen desde una perspectiva estratégica y no solamente técnica. b. Designar formalmente a una persona responsable de la seguridad y privacidad de la información mediante acto administrativo, conforme establecen los lineamientos regulatorios, asegurando que esta persona tenga las competencias, la experiencia y el respaldo institucional para cumplir con sus funciones. c. Incluir al Oficial de Seguridad de la Información como miembro con voz y voto en los comités institucionales de gestión y control interno, fortaleciendo su participación en la toma de decisiones y en el seguimiento de los riesgos.	**Plan de acción:** Presentar el hallazgo identificado sobre la ubicación del rol de Seguridad de la Información en la Subgerencia de TIC, junto con las recomendaciones emitidas por Control Interno, ante el Comité Institucional de Gestión y Desempeño. El objetivo es que dicho comité analice la situación y tome decisiones sobre la reubicación jerárquica del rol, garantizando su independencia, autonomía y alineación con los lineamientos establecidos en la Resolución 500 de 2021 del MINTIC. (Actualmente derogada por la Resolución MinTIC 02277 del 2025) **Responsable:** Subgerente de Tecnologías de la Información y las Comunicaciones. **Fecha Inicial:** 01-sep-2025 **Fecha Final:** 28-nov-2025

		La implementación de estas recomendaciones permitirá dotar de autonomía y relevancia estratégica al rol de Oficial de Seguridad de la Información, reduciendo riesgos y asegurando el cumplimiento de los lineamientos normativos vigentes.	
2.	**Gestión De Activos**		
2.1	**Disposición de los medios – Borrado seguro** Criterios: • ***"M1_TIC Manual de Políticas de Seguridad de la Información",*** *que establece:* *"Para los medios que contienen información confidencial, se deben almacenar y disponer de forma segura, mediante incineración, destrucción a través de máquinas destinadas para tal fin o proceso de borrado seguro, de acuerdo con las directrices de la Subgerencia de Gestión Administrativa y la Subgerencia de Tecnologías de la Información y las comunicaciones".* • ***MSPI - Modelo de Seguridad y Privacidad de la Información del MinTIC****, que establece la necesidad de proteger la información durante todo su ciclo de vida.* • ***ISO/IEC 27001:2013: Control A.8.3.2*** *Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.* • ***ISO/IEC 27001:2022: Control 8.10.*** *Establece la necesidad de eliminar información de forma segura antes de la disposición o reutilización de activos.*	Se recomienda acelerar la elaboración, formalización e implementación de un procedimiento para el borrado seguro de información en la infraestructura tecnológica de la Agencia, con el fin de garantizar la eliminación definitiva de datos sensibles, personales o confidenciales, especialmente en procesos de disposición, mantenimiento, reutilización o desincorporación de activos tecnológicos. Este procedimiento debe contemplar, entre otros, los siguientes aspectos: • Criterios de aplicabilidad por tipo de información y nivel de sensibilidad. • Métodos de borrado seguro (como sobreescritura, desmagnetización o destrucción física) según el tipo de medio de almacenamiento. • Registro y trazabilidad de las actividades de eliminación. • Roles y responsabilidades definidos para su ejecución y supervisión. • Tener en cuenta que a la fecha los equipos de cómputo que utilizan funcionarios y	**Plan de acción:** Documentar una guía técnica que establezca los lineamientos para la gestión del borrado seguro de información electrónica, garantizando su eliminación definitiva conforme a estándares de seguridad y normativas vigentes **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 11-ago-2025 **Fecha Final:** 30-dic-2025

	• ***ISO/IEC 27001:2022: Control 7.14.*** *Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia, han sido eliminados o sobrescritos de manera segura, antes de deshacerse de ellos o reutilizarlos.* • ***Ley 1581 de 2012: Protección de Datos Personales.*** *Exige medidas para evitar el acceso no autorizado a datos una vez finalizada su utilidad.* • ***Ley 1712 de 2014: Transparencia y Acceso a la Información Pública.*** *Requiere que la disposición final de documentos y medios respete la confidencialidad.* De acuerdo con la Matriz de Aplicabilidad, se encuentra pendiente la documentación y formalización del procedimiento que define las directrices y mecanismos para el **borrado seguro de información** en la infraestructura tecnológica aplicable. En esta Matriz no se observa responsables, entregables, ni fechas de implementación. Ver Anexo 1 La ausencia de un procedimiento específico de borrado seguro y/o disposición final de equipos, representa un riesgo para la confidencialidad y protección de los datos institucionales, especialmente en procesos de disposición, reutilización o desmantelamiento de activos tecnológicos, al no garantizar que la información sensible sea eliminada de manera definitiva y conforme a estándares de seguridad. Esta ausencia podría generar riesgos asociados a la seguridad, la trazabilidad y la protección de la información contenida en dichos equipos.	contratistas entran bajo la modalidad de arriendo. • Tener en cuenta que funcionarios y/o contratistas utilizan sus equipos personales.	

3.	Control De Acceso		
3.1	**Notificación de Credenciales** Criterios: • **ISO/IEC 27001:** Establece controles estrictos para la gestión segura de accesos, incluyendo la asignación individual de credenciales y su protección durante todo el ciclo de vida. • **Guía para la Gestión y Clasificación de Activos de Información (MINTIC):** …" *la gestión de activos debe estar alineada con el Dominio 8 Gestión de Activos del anexo A de la norma ISO 27001:2013, y la guía de controles del modelo de seguridad y privacidad de la información".* El Procedimiento "**P4_TIC Gestión de Acceso a Servicios Tecnológicos**", establece entre sus actividades, la notificación de información de autenticación secreta de la siguiente manera: *"9. El aplicativo envía automáticamente las credenciales de acceso al solicitante y al correo personal del nuevo funcionario o contratista".* Esta práctica compromete temporalmente la confidencialidad de la información, al ser divulgada la clave a una segunda parte.	Con relación a los lineamientos sobre autenticación, se recomienda modificar la actividad de notificación de las credenciales de acceso, garantizando que éstas sean entregadas únicamente a la persona autorizada que por sus funciones lo requiera, evitando su divulgación a otras partes, incluidos los niveles superiores.	**Plan de acción:** Modificar el procedimiento "P4_TIC Gestión de Acceso a Servicios Tecnológicos" para ajustar la actividad de notificación de credenciales, garantizando que la entrega de información de autenticación se realice únicamente al usuario autorizado, evitando su envío a correos personales u otras partes no involucradas directamente en el proceso. **Responsable:** Contratista ingeniero con obligaciones de infraestructura. **Fecha Inicial:** 01-ago-2025 **Fecha Final:** 19-dic-2025
3.2	**Administración de accesos y gestión de usuarios SICORE** Criterios: • ***NTC ISO/IEC 27001-2013: 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 a todo tipo de usuarios para todos los sistemas y servicios.*	Se recomienda implementar un módulo o funcionalidad integrada para la gestión de usuarios y administración de accesos en el sistema SICORE, que permita: a. Creación, modificación e inactivación de cuentas de usuario con trazabilidad.	**Plan de acción:** Definir con prioridades y criterios de aceptación establecidos por el área funcional, una funcionalidad centralizada de gestión de usuarios y accesos en SICORE; la Subgerencia TIC liderará el levantamiento de requerimientos

	• ***NTC ISO/IEC 27001-2022: 5.15 - Control de acceso:*** *Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información.* • ***M1_TIC Manual de Políticas de Seguridad de la Información - Política de control y gestión de acceso:*** *Se debe mantener un registro centralizado de los accesos suministrados.* Si bien, el sistema SICORE se encuentra en permanente actualización y mejora, actualmente no dispone de una funcionalidad o módulo centralizado para la administración de accesos y la gestión de usuarios, estas actividades se realizan previa solicitud y a través de scripts, lo cual representa una debilidad en el control de seguridad lógica y en la trazabilidad de acciones realizadas por los distintos perfiles.	b. Facilidad para la asignación de roles y perfiles según funciones del negocio. c. Parametrización de las directrices de seguridad para la autenticación. d. Registro de auditoría de accesos y actividades. Esta funcionalidad debe estar alineada con los principios de seguridad lógica, trazabilidad y mínimo privilegio establecidos en el MSPI.	mediante historias de usuario y el ciclo de análisis–diseño–implementación, incorporando creación/modificación. **Responsable:** Contratista ingeniero con obligaciones de líder de desarrollo de software **Fecha Inicial:** 02-feb-2026 **Fecha Final:** 15-dic-2026
3.3	**Matriz de Roles y Perfiles / Control de accesos** <u>Criterios:</u> • ***NTC ISO/IEC 27001-2013 - 9.4.1 - Derechos de acceso:*** *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.* • ***NTC ISO/IEC 27001-2022 - 5.18 - Derechos de acceso:*** *Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.* • ***NTC ISO/IEC 27002:2022 – 5.18.3: Asignación de derechos de acceso.*** *"Los derechos de acceso deben*	Se recomienda diseñar y formalizar la estructura de una "Matriz de roles y Perfiles" o "Matriz de Control de Accesos" que incluya el cruce detallado entre funcionalidades del sistema y los perfiles definidos, para ser diligenciada por parte de los dueños de proceso. Esta matriz debe contemplar, como mínimo: a. La descripción clara de cada rol funcional, sus responsabilidades y nivel de acceso requerido. b. La asignación específica de funcionalidades por perfil, asegurando el principio de mínimo privilegio.	**Plan de acción:** Diseñar e implementar un formato estandarizado de SICORE "Matriz de Roles y Perfiles / Control de Accesos" con modelo de datos (rol, responsabilidades, funciones habilitadas y nivel de acceso, funcional (dueños de proceso) para su definición, administración y actualización de roles. En el caso particular de SEVEN/KACTUS se validará la solicitud con respecto a la bolsa de horas

	asignarse de acuerdo con las necesidades del negocio, considerando los requisitos de seguridad de la información, y deben estar documentados y autorizados antes de su implementación." • ***PO1_TIC Política de Seguridad y Privacidad de la Información. Control de acceso:*** *La Subgerencia de Tecnologías de la Información y las Comunicaciones debe mantener actualizada la documentación relacionada con la administración de usuarios y monitoreará la asignación de permisos y roles otorgados a los usuarios.* . • ***M1_TIC Manual de Políticas de Seguridad de la Información - Política de control y gestión de acceso:*** o *El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas.* o *El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil asignado al usuario.* No se ha formalizado una "**Matriz de Roles y Perfiles**" o "**Matriz de Control de accesos**" aprobada por los responsables del proceso, para el acceso a los sistemas SICORE, SEVEN y KACTUS. Si bien, algunos roles han sido descritos en los criterios de aceptación de las historias de usuario, dentro del ciclo de desarrollo, no existe una estructura documental que permita visualizar de manera integral la asignación de funcionalidades por perfil. Esta ausencia limita la trazabilidad, la segregación de funciones y el control sobre los accesos y responsabilidades dentro del sistema.	c. La integración de esta matriz como documento de referencia en el ciclo de desarrollo, pruebas y despliegue del sistema, garantizando coherencia entre lo implementado y lo autorizado. d. La disponibilidad de la matriz para auditorías, como evidencia de control lógico y alineación normativa. e. La trazabilidad de aprobaciones, modificaciones y revisiones periódicas. La citada matriz es el instrumento técnico que permite cumplir con este requerimiento, conforme a los controles establecidos en el MSPI y la NTC-ISO/IEC 27000, facilitando la trazabilidad, la auditoría y la revisión periódica de privilegios.	**Responsable:** Contratista ingeniero con obligaciones de líder de desarrollo de software **Fecha Inicial:** 02-feb-2026 **Fecha Final:** 15-dic-2026

3.4	**Privilegios de los Usuarios de TICs** Criterios: • ***NTC ISO/IEC 27001-2013. A.6.1.2 Segregación de deberes:*** *Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.* • ***NTC ISO/IEC 27001-2022. 5.3 Segregación de deberes:*** *Los deberes y áreas de responsabilidad en conflicto deberían segregarse.* Los usuarios de la SUBGERENCIA TIC se encuentra asignados para el soporte técnico, operativo y funcional en los siguientes sistemas: **Sistema / Usuario / Rol / Grupo** SICORE: nbaron — SOPORTE SICORE: druiz — SOPORTE SICORE: jfherrera — SOPORTE SICORE: njimenez — SOPORTE SEVEN: acalderon — ADMINISTRADOR KACTUS: KADMATE — ADMINISTRADOR ATENEA Los usuarios con acceso al sistema SICORE con perfil “SOPORTE” asignados por la Subgerencia TIC, así como los usuarios “ADMINISTADOR” en los sistemas SEVEN y KACTUS, están habilitados para ejecutar actividades de parametrización y soporte, cuentan con privilegios para acceder a funcionalidades operativas y funcionales, lo que les permite realizar acciones como la adición, modificación y eliminación de información en módulos transaccionales o de negocio. La coexistencia de privilegios administrativos y operativos en un mismo perfil contraviene el principio de segregación de funciones, lo que podría facilitar la ejecución de actividades no autorizadas, dificultar la trazabilidad de eventos críticos y aumentar el riesgo de errores o fraudes no detectados.	Se recomienda revisar y ajustar los perfiles tipo “Administrador” y/o “Soporte” en los sistemas SICORE, SEVEN y KACTUS, con el fin de garantizar que no incluyan privilegios operativos, ni atributos que permitan la adición, modificación o eliminación de información relacionada con funciones del negocio. Estos perfiles deben limitarse exclusivamente a actividades de gestión de accesos, parametrización y soporte técnico. Para fortalecer el control de acceso y mitigar riesgos asociados a la falta de segregación de funciones, se sugiere: a. Implementar una clara segregación de funciones entre perfiles administrativos y operativos, evitando la superposición de responsabilidades. b. Establecer controles de acceso basados en el principio de mínimos privilegios, asignando únicamente los permisos estrictamente necesarios según el rol. c. Documentar y formalizar los perfiles de usuario, detallando sus permisos específicos y condiciones de uso. d. Realizar revisiones periódicas de los privilegios asignados, asegurando su trazabilidad y alineación con las funciones autorizadas.	**Plan de acción:** Realizar la revocación/ajuste técnico de permisos de los perfiles “Administrador/Soporte” en SICORE, SEVEN y KACTUS para eliminar privilegios operativos (alta/modificación/baja en módulos de negocio) y segregar funciones según mínimo privilegio; una vez ejecutado el cambio, emitir la comunicación a las áreas funcionales sobre la decisión en el marco de la auditoria. **Responsable:** Contratista seguridad de la información – Subgerente TICS **Fecha Inicial:** 02-feb-2026 **Fecha Final:** 15-dic-2026

4.	Seguridad De Las Operaciones		
4.1	**Registro de eventos (Logs de auditoría)** Criterios: • ***NTC ISO/IEC 27001-2013: A12.4.1 Registro de eventos:*** *"Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información".* • ***NTC ISO/IEC 27001-2013: A12.4.2 Protección de la información de registro:*** *"Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado".* • ***PO1_TIC Política de Seguridad y Privacidad de la Información. Seguridad de las Operaciones:*** *"Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información".* • ***M1_TIC Manual de Políticas de Seguridad de la Información. Política de registro y seguimiento de eventos de sistemas de información y comunicaciones:*** *"Los logs de eventos deben conservarse por un período mínimo de 6 meses y hasta 1 año para sistemas críticos o que involucren normativas de cumplimiento. Para logs operativos y de aplicaciones internas, el período de retención será de 1 año. En todos los casos, la eliminación de logs debe realizarse de manera segura conforme a las mejores prácticas de seguridad de la información".*	Se recomienda implementar las siguientes medidas: a. Ajustar la configuración de retención de logs tanto en la infraestructura de Oracle Cloud Infrastructure (OCI) como en los servidores backend WebLogic, de modo que se garantice el cumplimiento del periodo mínimo de conservación establecido por la política institucional. b. Implementar un procedimiento documentado para la eliminación segura de los logs, asegurando la trazabilidad y el alineamiento con las mejores prácticas en seguridad de la información. c. Implementar Mecanismos efectivos de registro y control que permitan evidenciar la revisión periódica de las actividades realizadas por los usuarios, para identificar excepciones, fallas y eventos de seguridad de la información, conforme a lo establecido en la "PO1_TIC Política de Seguridad y Privacidad de la Información".	**Plan de acción:** Determinar y documentar la factibilidad técnica y presupuestal de extender la retención de logs a 12 meses para SICORE, sin comprometer el presupuesto ni la continuidad operativa. **Responsable:** Contratista de la infraestructura – Subgerente TICS **Fecha Inicial:** 03-Nov-2025 **Fecha Final:** 15-Dic-2026

	a. Conservación registros de Eventos – Sistema SICORE Tiempo de conservación ○ Los registros deben guardarse como mínimo de 6 meses. ○ Para Logs operativos y los de aplicaciones internas o críticos (SICORE), se establece un período de 1 año. A la fecha, no se cuenta con registros de eventos con antigüedad superior a 6 meses o archivos mayores a 5 MB, lo que implica un incumplimiento del periodo de conservación según lo definido en el M1_TIC Manual de Políticas de Seguridad de la Información, específicamente en la Política de registro y seguimiento de eventos de sistemas de información y comunicaciones. **b. Revisión regular** Los soportes proporcionados sobre la revisión de las actividades realizadas por los usuarios corresponden a solicitudes de creación de usuarios y no constituyen evidencia según lo establece la "PO1_TIC Política de Seguridad y Privacidad de la Información: *"Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información"*. Ver Anexo 2.		

4.2	**Copias de Respaldo – Pruebas de restauración** Criterios: • ***NTC ISO/IEC 27001-2013: A.12.3.1 Respaldo de la información:*** *"Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada".* • ***M1_TIC Manual de Políticas de Seguridad de la Información.*** *Política de respaldo y restauración de información, que establece:* *"Los administradores de la plataforma de copias de respaldo de la entidad, mensualmente deben generar tareas de restauración aleatorias de la información de las bases de datos definidas por la Subgerencia de Tecnologías de la Información y las Comunicaciones, quedando registradas en el formato definido para tal fin; estas restauraciones deben ser documentadas, con el fin de garantizar la continuidad de las actividades realizadas en la Agencia, usando las herramientas tecnológicas en caso de presentarse la no disponibilidad de la información almacenada en las bases de datos".* No se aportaron los soportes sobre las pruebas de restauración que validan las copias de respaldo de las bases de datos de los diferentes sistemas de información, correspondientes a los meses de enero, febrero, marzo, abril y mayo de 2025, según lo requerido y establecido en el "Manual M1_TIC Políticas de Seguridad de la Información", específicamente en la Política de respaldo y restauración de información. Los documentos suministrados únicamente acreditan los ejercicios de restauración realizados en el marco del Plan de Recuperación de Desastres de SIGA efectuadas en junio 2025.	Se recomienda implementar un procedimiento formal y documentado para la realización, control y almacenamiento de los soportes correspondientes a las pruebas de restauración de las copias de respaldo de las bases de datos de los diferentes sistemas de información. Este procedimiento debe garantizar: a. Que, para cada mes y cada sistema, se conserven evidencias claras y verificables de las pruebas efectuadas, en cumplimiento de lo dispuesto en el "Manual M1_TIC Políticas de Seguridad de la Información", específicamente en la Política de respaldo y restauración de información. b. Revisiones periódicas al proceso, a fin de asegurar la trazabilidad y disponibilidad de los soportes requeridos durante auditorías o revisiones de control interno.	**Plan de acción:** No aplica plan de acción para este hallazgo **Responsable:** No aplica **Fecha Inicial:** No aplica **Fecha Final:** No aplica **NOTA:** El procedimiento "**G4_TIC Guía Institucional Copias de Seguridad (Oracle Cloud y Microsoft 365**)" fue aprobado el 1-jul-25 y radicado el 22-jul-25, durante el desarrollo de la auditoría. Se reporta como una Mejora subsanada.

5.	Adquisición, Desarrollo Y Mantenimientos De Sistemas		
5.1	**Control de Cambios** Criterios: • **"M1_TIC Manual de Políticas de Seguridad de la Información"**: *"Definir y documentar la gestión de cambios en las instalaciones de procesamiento de información y los sistemas de información".* • ***NTC ISO/IEC 27001:2013 / 2022*** *- **A.12.1.2**: Se deben controlar los cambios en instalaciones de procesamiento de información.* *- **A.14.2.2**: Requiere procedimientos formales para la gestión de cambios en sistemas.* En la validación efectuada a la Política de Seguridad de la Información y a los procedimientos referentes a las definiciones relacionadas con el **Control de Cambios**, evidenciamos lineamientos generales relacionados con esta práctica. No obstante, según la "Matriz de Aplicabilidad ATENEA 2025", y la validación de los procedimientos publicados al 31-jul-25, la entidad no cuenta, con un procedimiento formalmente documentado que defina las actividades, roles y responsabilidades para el Control de cambios en los sistemas de información. Ver Anexo 3. Situación que representa un incumplimiento frente a lo establecido en el **Manual de Políticas de Seguridad de la Información.** Igualmente, la Matriz de Aplicabilidad, no cuenta con Plan de acción, responsables, entregables, así como fecha de implementación.	Agilizar la documentación, formalización e implementación del procedimiento de Control de Cambios aplicable a los sistemas de información institucionales. Este procedimiento debe contemplar, como mínimo, los siguientes aspectos: **a. Clasificación de cambios:** Definir los criterios para categorizar los cambios. Ejemplo: ○ *Estándar:* Cambios rutinarios, preaprobados y de bajo riesgo. ○ *Normal:* Cambios que requieren evaluación, aprobación y planificación. ○ *Emergencia:* Cambios urgentes que deben aplicarse para mitigar incidentes críticos o vulnerabilidades. **b. Evaluación de riesgos e impacto:** Incorporar un análisis formal que permita: ○ *Identificar riesgos técnicos, operativos y de seguridad* ○ *Evaluar el impacto en la disponibilidad, integridad y confidencialidad de la información* ○ *Determinar medidas de mitigación* **c. Definición de roles y responsabilidades:** Identificar y asignar funciones específicas dentro del proceso, tales como: ○ *Solicitante del cambio* ○ *Evaluador técnico*	**Plan de acción:** Actualizar el procedimiento P7_TIC Gestión de Cambios en Infraestructura Tecnológica, para integrar la gestión de cambios en los sistemas de información institucionales **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 01-Sep-2025 **Fecha Final**: 30-Ene-2026 **NOTA:** El procedimiento "P7_TIC Gestión Cambios Infraestructura Tecnológica", fue aprobado el 15-jul-25 y suministrado el 01-ago-2025 durante el desarrollo de la auditoría, por lo cual se reporta como una oportunidad de Mejora Subsanada.

		○ *Comité de cambios (CAB)* ○ *Aprobador final* ○ *Responsable de implementación y seguimiento* **d. Mecanismos de reversión y comunicación:** ○ *Definir planes de reversión (roll-back) ante fallos en la implementación* ○ *Establecer canales y formatos para comunicar los cambios a usuarios, áreas afectadas y partes interesadas.* **e. Registro y trazabilidad:** Utilizar herramientas como la Mesa de Ayuda para garantizar: ○ *Registro estructurado de cada solicitud de cambio* ○ *Seguimiento del ciclo de vida del cambio* ○ *Evidencia de aprobaciones, pruebas y resultados* **f. Matriz de Aplicabilidad:** Completar y mantener actualizada la matriz, relacionando el Plan de acción, responsables, entregables, así como fecha de implementación.	

5.2	**Desarrollo seguro** Criterios: • ***NTC ISO/IEC 27001-2013: A.14.2.1 – Política de desarrollo seguro:*** *Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.* • ***NTC ISO/IEC 27001-2013: A.14.2.5 – Principios de construcción de 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.* • ***NTC ISO/IEC 27001-2022: 8.25 – Ciclo de vida de desarrollo seguro:*** *Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas* • ***M1_TIC Manual de Políticas de Seguridad de la Información.*** o *Definir y documentar los requisitos de seguridad para la adquisición, desarrollo de los sistemas y mejoras de los existentes.* o *"El desarrollo de aplicativos o sistemas de información diseñado por terceros debe estar bajo estándares de desarrollo de la Subgerencia de Tecnologías de la Información y las Comunicaciones y alineado a las políticas de seguridad de la información".* En la revisión de las definiciones relacionados con "Política de desarrollo seguro" y "Principios de construcción de sistemas seguros", se evidenció que la entidad cuenta con Políticas y procedimiento formalizado de desarrollo y mantenimiento de sistemas de información, el cual define las actividades necesarias	Se recomienda formalizar un procedimiento específico para el desarrollo seguro de aplicaciones y sistemas de información, que incluya, como mínimo: a. Definición clara de reglas, estándares y lineamientos técnicos basados en buenas prácticas internacionales. b. Incorporación de principios de seguridad desde las etapas iniciales del ciclo de vida del software (seguridad desde el diseño). c. Establecimiento de una arquitectura general que contemple requisitos mínimos de seguridad para aplicaciones y sistemas institucionales. Adicionalmente, se sugiere actualizar la Matriz de Aplicabilidad 2025, registrando los campos de "Responsable", "Estado de Entregables" e incluir una fecha de Implementación, con el fin de facilitar el monitoreo, trazabilidad y seguimiento efectivo de este control.	**Plan de acción:** Definir, documentar y socializar lineamientos de desarrollo seguro que incluyan estándares mínimos y principios de seguridad desde el diseño. **Responsable:** Contratista ingeniero con obligaciones de líder de desarrollo de software **Fecha Inicial:** 02-Feb-2026 **Fecha Final:** 31-Jul-2026

	para planificar, administrar y verificar las fases del ciclo de vida del software. Sin embargo, de acuerdo con lo establecido en la Matriz de Aplicabilidad 2025: • No se ha documentado un procedimiento específico que defina reglas, estándares o lineamientos técnicos para el desarrollo seguro de aplicaciones y sistemas. • Tampoco se ha establecido una arquitectura general que incorpore principios de seguridad desde la etapa de diseño y construcción, conforme a las buenas prácticas en desarrollo seguro. Por otra parte, la Matriz de Aplicabilidad, no presenta información en los campos: "Responsable", "Estado de Entregables", así como la "Fecha de Implementación", lo que limita el seguimiento y control efectivo de este componente. Ver Anexo 4.		
5.3	**Datos de Prueba** Criterios: • ***NTC ISO/IEC 27001-2013: A.14.3.1 – Protección de datos de prueba:*** *"Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente".* • ***NTC ISO/IEC 27001-2022: 8.33 – Datos de Prueba.*** *Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados".* • ***M1_TIC Manual de Políticas de Seguridad de la Información.*** o *"Asegurar que las bases de datos utilizadas en ambientes de prueba sobre las etapas de desarrollo de soluciones de información no corresponden a información real o la misma debe ser modificada para tales fines".*	Acelerar la definición e implementación de las siguientes medidas de control: a. Adoptar tecnologías y procesos que permitan anonimizar o enmascarar los datos cuando sea imprescindible utilizar información similar a la real, garantizando que no sea posible la re-identificación de personas. b. Documentar y monitorear las actividades relacionadas con la generación, uso y eliminación de datos de prueba, estableciendo revisiones internas regulares que permitan validar el cumplimiento de la normatividad y las políticas internas de la Agencia. c. Capacitar periódicamente al personal involucrado en el ciclo de vida del desarrollo	**Plan de acción:** Documentar en la Matriz de Aplicabilidad cómo se ejecuta el control de protección de datos de prueba, especificando criterio de aplicabilidad. **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 03-Mar-2026 **Fecha Final:** 15-Dic-2026

	○ *"Los datos de prueba no deben contener datos personales o información sensible, de ser necesario este contenido se deben utilizar mecanismos de enmascaramiento o sustitución de datos".* En la validación realizada sobre los "Datos de Prueba", se evidenció la existencia de lineamientos y procedimientos orientados a su protección. Sin embargo, conforme a lo señalado en la Matriz de Aplicabilidad, aún no se han implementado controles específicos sobre los Datos de Prueba. Ver Anexo 5. Por otra parte, la Matriz de Aplicabilidad, no presenta información en los campos: "Responsable", "Estado de Entregables", así como la "Fecha de Implementación", lo que limita el seguimiento y control efectivo de este componente.	de software sobre la importancia de la protección de los datos de prueba y la responsabilidad frente a la privacidad y la seguridad. La adopción de estos controles fortalece la protección de los datos personales y contribuye al cumplimiento de las obligaciones legales.	

No.	OPORTUNIDAD DE MEJORA	RECOMENDACIÓN	PLAN DE ACCIÓN
1.	**Políticas De Seguridad De La Información**		
1.1	**Excepción, desviación y sanciones** Durante la revisión realizada a la "PO1_TIC Política de Seguridad y Privacidad de la Información", V2 aprobada el 21/11/2024", en relación con las disposiciones sobre "excepciones, desviaciones y sanciones", se identificó que únicamente el capítulo "4.1. Roles y Responsabilidades" asigna a la "Oficina de Control Interno Disciplinario" la responsabilidad de investigar los incumplimientos a las Políticas definidas. No se encontraron lineamientos adicionales que precisen los tipos de excepciones y/o desviaciones.	La Política de Seguridad de la Información debe contemplar, entre otros, los siguientes aspectos: Definición de excepciones: Especificar en qué circunstancias una norma, directriz o medida establecida no aplicaría y/o especificar que no hay excepciones. La Oficina de Control Interno Disciplinario, será responsable de tomar las decisiones pertinentes y de determinar la sanción o amonestación que corresponda en cada caso.	**Plan de acción:** Incluir en el Manual de Políticas de Seguridad de la Información (M1_TIC) el tratamiento de excepciones frente al cumplimiento de las directrices del SGSI. **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 12-Nov-2025 **Fecha Final:** 30-Jun-2026
1.2	**Socialización de la Política de Seguridad** Criterios: **PO1_TIC Política de Seguridad y Privacidad de la Información. "Formación y Concientización":** *"Todos los funcionarios, contratistas y cualquier persona que tenga acceso a los recursos tecnológicos deben estar al tanto de las políticas, normativas y procedimientos relacionados con la seguridad de la información".* Durante la revisión sobre la socialización de la Política de Seguridad de la Información, se evidenció que, aunque esta se encuentra publicada en la página oficial de ATENEA https://www.agenciaatenea.gov.co y se difunden "Cápsulas de Saberes" o "piezas gráficas" con recomendaciones sobre seguridad de la información, no existen pruebas que acrediten que	Se recomienda fortalecer la socialización de la Política de Seguridad de la Información, asegurando que todo el personal vinculado a la entidad (funcionarios y contratistas), así como personas externas con acceso a recursos tecnológicos, conozcan y comprendan plenamente las políticas, normativas y procedimientos relacionados con la seguridad de la información. Para garantizar este objetivo, la entidad debe considerar: a. Complementar las estrategias de capacitación y sensibilización, que incluyan registros de asistencia y evaluaciones para	**Plan de acción:** Ejecutar y mantener evidencia de socialización de la Política de Seguridad de la Información, que incluya registros de asistencia, materiales utilizados (como piezas gráficas y presentaciones). **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 01-Jun-2025 **Fecha Final:** 23-Dic-2025

	todo el personal (funcionarios y contratistas) conocen efectivamente la política.	evidenciar el conocimiento adquirido por cada persona. b. Dejar constancia documental, accesible para auditorías, donde se registre la participación y comprensión del personal respecto a la política. c. Actualizar y difundir, de manera proactiva, cualquier cambio en la normativa interna relacionada con la seguridad de la información. De esta manera, se fortalece la cultura organizacional en materia de seguridad de la información y se da cumplimiento a la normatividad vigente del sector público colombiano.	
2.	**Responsabilidades Y Organización Seguridad Información**		
2.1	**Gestión del Riesgo de Seguridad de la Información** En la validación realizada a la Política de Seguridad de la Información, se observa que, no se mencionan de manera explícita las directrices con la **"Política de Riesgos Gestión, Corrupción, Fiscales, Seguridad Digital y LA/FT**" del Proceso de Direccionamiento Estratégico, siendo ésta la base de aquella.	Se recomienda fortalecer y actualizar la Política de Seguridad de la Información, integrando de manera explícita la gestión de riesgos institucional o, estableciendo referencias claras y precisas a dicha gestión. Esta actualización debe asegurar que las directrices de las diferentes Políticas estén alineadas entre sí, garantizando la coherencia en los criterios de aceptación del riesgo y la adecuada administración del riesgo residual. Lo anterior, teniendo en cuenta que la Política de Seguridad de la Información se desarrolla y actualiza en cada vigencia, de acuerdo con los riesgos, los requerimientos institucionales y la normatividad.	**Plan de acción:** Actualizar la Política de Seguridad de la Información incluyendo una sección que establezca la alineación con las directrices institucionales definidas en la Política de Riesgos Institucional (Gestión, Corrupción, Fiscales, Seguridad Digital y LA/FT) **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 12-Nov-2025 **Fecha Final:** 30-Jun-2026

2.2	**Segregación de funciones** Como resultado de la validación sobre la "Segregación de funciones", se identificó que la Política de Seguridad de la Información y sus documentos complementarios establecen controles para la administración de usuarios, así como mecanismos de monitoreo en la asignación de permisos y roles. Al respecto, no se evidenció un lineamiento claro y específico sobre la segregación de funciones y áreas de responsabilidad, orientado a evitar que una sola persona pueda asumir funciones potencialmente conflictivas dentro de los procesos.	Incorporar en la Política de Seguridad de la Información o documentos anexos, directrices explícitas sobre la segregación de funciones, definiendo claramente las responsabilidades y los límites de acceso para cada cargo o área. Esto permitirá reducir el riesgo de error, fraudes o accesos indebidos, garantizando que ninguna persona tenga la posibilidad de operar de manera autónoma en actividades críticas sin la debida supervisión o autorización.	**Plan de acción:** Actualizar el Manual de Seguridad de la Información incorporando lineamientos sobre la segregación de funciones, definiendo responsabilidades diferenciadas para cada rol o área. **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 12-Nov-2025 **Fecha Final:** 30-Jun-2026
2.3	**Inteligencia de amenazas** <u>Criterios:</u> • ***ISO/IEC 27002:2022 – Control 5.7*** *Recomienda establecer procesos formales para la inteligencia de amenazas, incluyendo fuentes, análisis, difusión y respuesta* • ***MSPI - Modelo de Seguridad y Privacidad de la Información*** *Promueve la gestión proactiva de riesgos, incluyendo el análisis de amenazas como parte del ciclo de mejora continua del SGSI.* Aunque la Agencia dispone de fuentes externas de contacto con grupos de interés especializados en seguridad de la información, herramientas como Darktrace para el monitoreo del tráfico y la recepción oportuna de alertas y vulnerabilidades, no se evidencian lineamientos ni procedimientos formalmente documentados que	Se recomienda establecer un procedimiento formal para la recopilación, análisis y gestión de información relacionada con amenazas. Este procedimiento debe estar alineado con las definiciones del Modelo de Seguridad y Privacidad de la Información (MSPI) del (MinTIC), así como con las mejores prácticas internacionales, como las definidas en la norma ISO/IEC 27001. La implementación de un proceso estructurado de inteligencia de amenazas permitirá: • Identificar patrones y tendencias que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional. • Facilitar la toma de decisiones informadas en la gestión de riesgos tecnológicos.	**Plan de acción:** Actualizar el M1_TIC Manual de Políticas de Seguridad de la Información, con el fin de incorporar una política sobre inteligencia de amenazas, alineada con el MSPI y la norma ISO/IEC 27002:2022, ya sea como parte de la gestión de vulnerabilidades o como un componente independiente, que defina los lineamientos para la recolección, análisis y uso de información relevante para la detección proactiva de amenazas de acuerdo con las herramientas tecnológicas disponibles en la entidad.

	regulen el análisis de dicha información en el contexto de amenazas. Esta ausencia podría limitar la consistencia y efectividad en la identificación de tendencias y la gestión proactiva de riesgos.	• Cumplir con los principios de responsabilidad, trazabilidad y prevención establecidos en la normatividad vigente para entidades públicas. Se sugiere que dicho procedimiento incluya fuentes internas y externas de información, criterios de priorización, roles y responsabilidades, así como mecanismos de documentación y retroalimentación.	**Responsable:** Contratista seguridad de la información **Fecha Inicial:** 01-Oct-2025 **Fecha Final**: 30-Mar-2026
3.	**Control De Acceso**		
3.1	**Autorización en el suministro de acceso** En la evaluación realizada a "**P4_TIC Procedimiento Gestión De Acceso A Servicios Tecnológicos"** se identificaron actividades y definiciones orientados a la gestión de accesos a los usuarios; no obstante, se evidenció la ausencia de una referencia clara a la participación del **propietario del activo de información** como responsable de autorizar los accesos a los activos de información. La PO1_TIC Política de Seguridad y Privacidad de la Información, define: *"**Propietario de activo de información**: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados".*	Actualizar las responsabilidades de los propietarios de los activos de información, el cual debe entre otras funciones, establecer los requisitos de seguridad de la información y control de acceso. Algunas de sus funciones que debe asumir son: • Definir qué usuarios pueden tener permisos de acceso a la información de acuerdo con sus funciones y competencia. • Autorizar las solicitudes de acceso a los sistemas de información.	**Plan de acción:** Actualizar el Manual de Seguridad de la Información para formalizar la participación del propietario del activo de información como responsable de autorizar el suministro de accesos a sistemas o activos bajo su custodia, en concordancia con la definición establecida en la Política de Seguridad. **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 12-Nov-2025 **Fecha Final:** 30-Jun-2026

3.2	**Revisiones de los administradores funcionales** Criterios: • "**M1_TIC Manual de Políticas de Seguridad de la Información**", que establece: *"Los administradores funcionales de los sistemas de información deben realizar revisiones periódicas por lo menos una semestral de los usuarios activos en los diferentes sistemas de información, dominio y red".* • **NTC ISO/IEC 27001-2013:** ***A.9.2.5 – Revisión de derechos de acceso de usuarios:*** *Requiere que se revisen regularmente los derechos de acceso de los usuarios para asegurar que sean apropiados.* • **NTC ISO/IEC 27001-2022:** ***5.18. Derechos de acceso:*** *Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.* Como resultado de la verificación efectuada sobre el registro, cancelación de usuarios y cambio de rol, se observó la existencia de lineamientos de seguridad que regulan dichos procesos. Sin embargo, respecto a las revisiones semestrales que deben realizar los responsables de la administración funcional de los sistemas de información, no se observaron: • Evidencias que respalden los resultados de las revisiones realizadas. • La aplicación de estas revisiones en los distintos sistemas de información o se carece de documentación o registro formal.	Se recomienda establecer un cronograma formalizado y documentado, o lista de chequeo, para la realización de las revisiones de los usuarios en los sistemas de información. Este procedimiento debe incluir: • La elaboración de un registro detallado de cada revisión, especificando los sistemas revisados, los responsables, las actividades realizadas y los resultados obtenidos. • La implementación de controles que aseguren la aplicación de la revisión en todos los sistemas de información administrados y con la periodicidad definida. • La designación de responsables para el seguimiento y validación de las evidencias generadas durante la revisión. La adopción de estas medidas permitirá fortalecer la trazabilidad del proceso, garantizar el cumplimiento de lo establecido y fomentar la mejora continua en los controles internos de los sistemas de información.	**Plan de acción:** Establecer y documentar un cronograma de revisiones semestrales por parte de los administradores de los sistemas de información, incluyendo responsables y sistemas revisados. **Responsable:** Contratista seguridad de la información **Fecha Inicial:** 01-Sep-2025 **Fecha Final**: 30-Ene-2026

4.	**Seguridad De Las Comunicaciones**		
4.1	**Acuerdos de confidencialidad o de no divulgación** Criterios: • ***NTC ISO/IEC 27001-2013: A.13.2.4 – Acuerdos de confidencialidad o de no divulgación:*** *"Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información".* • ***NTC ISO/IEC 27001-2022: 6.6 – Acuerdos de confidencialidad o no divulgación:*** *"Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la información de la organización deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes".* • ***PO1_TIC Política de Seguridad y Privacidad de la Información*** *"Incorporar en el modelo de los contratos clausulas y obligaciones, sobre el cumplimiento de las políticas de seguridad, privacidad y confidencialidad sus procedimientos y los acuerdos de confidencialidad correspondientes".* • ***M1_TIC Manual de Políticas de Seguridad de la Información.*** *"Los acuerdos contractuales deben establecer la responsabilidad del colaborador en cuanto a seguridad de la información -derechos de autor, confidencialidad y no divulgación de la información durante y después del empleo".* Se evidenció la existencia de políticas y directrices que regulan los acuerdos de confidencialidad o no divulgación para la protección	Se recomienda formalizar el uso de acuerdos de confidencialidad individuales, suscritos por funcionarios, practicantes con acceso a información institucional sensible, con el fin de fortalecer la trazabilidad y el cumplimiento normativo en materia de protección de datos y reserva documental. Para ello, se sugiere: a. Diseñar e implementar un formato estándar de acuerdo de confidencialidad, alineado con la normatividad vigente y aprobado por la oficina jurídica. b. Integrar dicho formato como parte del proceso de vinculación, inducción o asignación de funciones. c. Registrar en la Matriz de Aplicabilidad los siguientes campos: Responsable, Estado de Entregables, y Fecha de Implementación, para garantizar el control operativo y cumplimiento de entregables. Esta medida contribuirá a consolidar la gestión responsable de la información institucional, y mitigar riesgos asociados al uso indebido o divulgación no autorizada de información.	**Plan de acción:** Gestionar con la Oficina Jurídica y Subgerencia Administrativa la definición e implementación de un formato estándar de acuerdo de confidencialidad, alineado con la normativa vigente, para su incorporación en los procesos de vinculación, contratación e inducción de funcionarios y contratistas con acceso a información sensible. Desde la Subgerencia TICS se apoyará este proceso aportando los requerimientos técnicos de seguridad de la información y realizando el seguimiento en la Matriz de Aplicabilidad para asegurar la trazabilidad y el cumplimiento. **Responsable:** Subgerente TICS Contratista de seguridad de la información **Fecha Inicial:** 01-Oct-2025 **Fecha Final:** 30-Ene-2026

	de la información en contratos de prestación de servicios. Sin embargo, según lo establecido en la Matriz de Aplicabilidad, no se cuenta con un formato de confidencialidad formalmente definido y firmado de manera individual para funcionarios y practicantes. Por otro lado, la Matriz no registra la información correspondiente a los campos: "Responsable", "Estado de Entregables" ni la fecha de implementación. Ver Anexo 6.		
5.	**Adquisición, Desarrollo Y Mantenimientos De Sistemas**		
5.1	**Especificaciones de los requisitos de seguridad de la información** Criterios: • ***NTC ISO/IEC 27001-2013: 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.* • ***M1_TIC Manual de Políticas de Seguridad de la Información.*** *"Definir y documentar los requisitos de seguridad para la adquisición, desarrollo de los sistemas y mejoras de los existentes".* Como resultado de la validación realizada sobre el "Análisis y especificación de requisitos de seguridad de la información", se identificó la existencia de políticas, directrices y procedimientos que orientan la presentación de los requerimientos de desarrollo. Sin embargo, se observó que el formato "f1_p5_tic_historia_de_usuario_v1" no incluye campos que aseguren la consideración de las especificaciones de seguridad en todos los casos.	Se recomienda actualizar el formato "f1_p5_tic_historia_de_usuario_v1" para incluir campos específicos que permitan registrar de manera clara y estructurada los requisitos de seguridad de la información. Esta mejora garantizaría que, en cada caso, se consideren aspectos de seguridad, entre otros, como: • ¿Aplica cifrado? • ¿Requiere autenticación? • ¿Debe registrarse evento en el log de auditoría? • Restricciones de acceso Fortaleciendo así, el cumplimiento de las políticas y procedimientos en materia de seguridad.	**Respuesta SubTIC:** No se acoge la oportunidad de Mejora.

6.	Continuidad De Negocio		
6.1	**Relación de proveedores en DRP** Criterios: • ***NTC ISO/IEC 22301:2019: Sistema de gestión de continuidad de negocio.*** ***4.2 – Comprensión de las necesidades y expectativas de las partes interesadas - Relación con proveedores:*** *"Implica documentar qué servicios dependen de terceros y cómo se garantiza su disponibilidad durante una interrupción".* ***8.3 – Planes y procedimientos de continuidad del negocio - Relación con proveedores:*** *"Deben incluirse matrices de contacto de proveedores, responsables asignados y canales de comunicación".* En la revisión del Plan de Recuperación ante Desastres (DRP), no se evidenció: • Información que identifique a los proveedores vinculados a cada uno de los servicios críticos de Informática. • Matriz de contacto que consolide los datos de los proveedores de servicios externos. Lo anterior, limita la capacidad de respuesta coordinada ante incidentes que requieran su intervención.	Se recomienda actualizar el DRP considerando: a. Una matriz de servicios críticos que relacione cada servicio con su proveedor correspondiente. b. Una matriz de contacto de proveedores, que incluya nombre de a empresa, responsable asignado, canales de comunicación, horarios de atención y acuerdos de nivel de servicio (SLA). c. Un procedimiento de verificación y actualización periódica de esta información, alineado con los controles de continuidad del negocio establecidos en ISO 22301 e ISO 27001:2022. Esta mejora fortalecerá la trazabilidad, la capacidad de respuesta y la resiliencia institucional ante eventos disruptivos.	**Plan de acción:** Construir el Anexo "Relación y Contactos de Proveedores Críticos", que incluya: matriz de servicios críticos vs. Proveedor y matriz de contacto (empresa, responsable, canales, horarios de atención) **Responsable:** Contratista oficial de seguridad **Fecha Inicial:** 02-Feb-2026 **Fecha Final:** 29-May-2026

6.2	**Pruebas al Plan de recuperación ante Desastres** Criterios: • ***NTC ISO/IEC 27001-2013: 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.* • ***M1_TIC Manual de Políticas de Seguridad de la Información****: Se debe desarrollar e implementar un Plan de recuperación de TI, para asegurar que los procesos misionales de TI de la Agencia, los cuales serán restaurados dentro de escalas de tiempo razonables. El plan de acción que permitirá la recuperación de los servicios de TI, se desarrollará teniendo en cuenta los siguientes aspectos:* o *Identificación y asignación de prioridades a los procesos críticos de TI de la Agencia de acuerdo con su impacto en el cumplimiento de la misión de la entidad.* o *Documentación de la estrategia de continuidad TI.* o *Documentación del plan de recuperación de TI, de acuerdo con la estrategia definida anteriormente.* o *Plan de pruebas para la estrategia de recuperación de los servicios de TI.* En la validación de las pruebas realizadas al Plan de Recuperación ante Desastres (DRP), con base en los siguientes documentos: a. Acta de Reunión. Correspondiente a Ejecución de las pruebas del Plan de Recuperación ante Desastres para el Portal Web y la Intranet. Ver Anexo 7.	Se recomienda fortalecer la documentación técnica y operativa de las pruebas realizadas al Plan de Recuperación ante Desastres (DRP), incorporando los elementos clave que permitan evidenciar la planificación, ejecución, evaluación y retroalimentación del ejercicio. Para ello, se sugiere: a. Implementar un **formato estandarizado** para el registro de pruebas del DRP, que incluya fecha, lugar, duración, participantes, roles, escenario de prueba, indicadores, resultados obtenidos, incidentes detectados, análisis comparativo y propuestas de mejora. b. Asegurar que los resultados de las pruebas estén vinculados con los objetivos del DRP y con el análisis de riesgos vigente. c. Incluir recomendaciones técnicas y organizativas, así como acciones correctivas y fechas de seguimiento. d. Documentar los riesgos residuales identificados y si corresponde, definir la necesidad de actualizaciones al DRP o a sus anexos. Estas acciones permitirán mejorar la trazabilidad del proceso, facilitar auditorías internas y externas, y fortalecer la resiliencia institucional ante eventos disruptivos.	**Plan de acción:** Implementar un formato estandarizado para documentar las pruebas del DRP **Responsable:** Contratista oficial de seguridad **Fecha Inicial:** 02-Feb-2026 **Fecha Final:** 29-May-2026

	b. Seguimiento plan de riesgos relacionados con Disaster Recovery Plan para la infraestructura tecnológica de la entidad. Ver Anexo 8. Se identificó que la documentación analizada no incluye información esencial para evidenciar la planeación, ejecución y análisis de las pruebas, como: • Fecha, lugar y duración • Participantes y roles involucrados • Tiempos de respuesta frente a lo planeado • Incidentes detectados o desviaciones durante la ejecución • Comparación contra objetivos definidos • Recomendaciones técnicas y organizativas • Riesgos residuales si los hay • Necesidad de actualizaciones al plan o documentación relacionada • Acciones correctivas asignadas • Fechas previstas para implementación • Próxima fecha de prueba o revisión La ausencia de estos elementos limita la trazabilidad del ejercicio, impide verificar su efectividad y dificulta la formulación de mejoras continuas al DRP.		

ANEXOS

Anexo 1

Número de Control	Control	Estado Control	Evidencia
7.14	Eliminación o reutilización segura de equipos	Implementado parcialmente	La entidad cuenta con procedimientos formales para el control, baja y disposición final de activos fijos, incluyendo equipos de cómputo, bajo aprobación del Comité Institucional de Gestión y Desempeño, con conceptos técnicos de la Subgerencia TIC.

Número de Control	Control	Requiere Mejoras	Plan de Acción
7.14	Eliminación o reutilización segura de equipos	Si	Documentar y formalizar la guia de borrado seguro de información en la infraestructura tecnológica aplicable

Anexo 2

SOLICITUD CREACION USUARIOS Y CONTRASEÑAS IES

Desde Carolina Sepúlveda Garcia <csepulveda@agenciaatenea.gov.co>
Fecha Mar 10/06/2025 15:31
Para Juan Fernando Herrera Martínez <jfherrera@agenciaatenea.gov.co>; Maria Alejandra Cano Martinez <mcano@agenciaatenea.gov.co>
CC Carlos Andres Ballesteros Castañeda <cballesteros@agenciaatenea.gov.co>; Andrea Marcela Jimenez Lopez <ajimenez@agenciaatenea.gov.co>

1 archivo adjunto (15 KB)
Asignación de usuario IES cargue de información en sistema VF.xlsx;

Estimados,

Cordial saludo.

En el marco de las responsabilidades asignadas al equipo de Supervisión Posmedia, me permito solicitar la creación de usuarios y contraseñas para el acceso a la plataforma SICORE, de las Instituciones de Educación Superior

Adjunto a este correo encontraran la base de datos con la información de las personas responsables, incluyendo su correo institucional y las instituciones de educación superior.

Quedo atenta cualquier información adicional que se requiera.

SOLICITUD CREACION USUARIOS Y CONTRASEÑAS INSTITUCIONES ETDH

Desde Carolina Sepúlveda Garcia <csepulveda@agenciaatenea.gov.co>
Fecha Vie 11/07/2025 16:30
Para Juan Fernando Herrera Martínez <jfherrera@agenciaatenea.gov.co>; Maria Alejandra Cano Martinez <mcano@agenciaatenea.gov.co>
CC Carlos Andres Ballesteros Castañeda <cballesteros@agenciaatenea.gov.co>; Andrea Marcela Jimenez Lopez <ajimenez@agenciaatenea.gov.co>

1 archivo adjunto (13 KB)
Asignación de usuario IES cargue de información en sistema 1.xlsx;

Estimados,

Cordial saludo.

En el marco de las responsabilidades, me permito solicitar la creación de usuarios y contraseñas para el acceso a la plataforma SICORE, de las Instituciones de Educación de ETDH.

Adjunto a este correo encontraran la base de datos con la información de las personas responsables, incluyendo su correo institucional y las instituciones de educación superior.

Quedo atenta cualquier información adicional que se requiera.

RE: Insumos Alistamiento Piloto Formalización

Desde Andrea Marcela Jimenez Lopez <ajimenez@agenciaatenea.gov.co>
Fecha Mar 25/03/2025 16:05
Para Juan Fernando Herrera Martínez <jfherrera@agenciaatenea.gov.co>
CC Carlos Andres Ballesteros Castañeda <cballesteros@agenciaatenea.gov.co>; Rubith Ofir Tuberquia Avendaño <rtuberquia@agenciaatenea.gov.co>; Carlos Cardenas Perez <cacardenasp@agenciaatenea.gov.co>; Silvia Liliana Londoño Castaño <slondono@agenciaatenea.gov.co>; Maria Alejandra Cano Martinez <mcano@agenciaatenea.gov.co>; Milena Delgado Hernández <mdelgado@agenciaatenea.gov.co>; Alba Sofia Monroy Galvis <amonroy@agenciaatenea.gov.co>; Ana Carolina Alonso Ramirez <aalonso@agenciaatenea.gov.co>

Hola Juan Fernando,

En respuesta a tu solicitud, te comparto la relación de los usuarios definidos hasta la fecha, con el fin de avanzar en la creación de lo necesario para el correcto desarrollo del pilotaje.

Para el ambiente productivo de cada una de las cuatro IES participantes (Pedagógica, Distrital, ETITC y SENA), se han asignado los mismos roles en cada institución, de la siguiente manera:

- **Rol Apoyo a la Supervisión Posmedia:**
  Nombre: Andrea Marcela Jiménez López
  Tipo y número de documento: CC 1065657464
  Correo: ajimenez@agenciaatenea.gov.co
- **Rol Articulador Posmedia:**
  Nombre: Alba Sofía Monroy Galvis
  Tipo y número de documento: CC 35253862
  Correo: amonroy@agenciaatenea.gov.co
- **Rol Apoyo Jurídico Posmedia:**
  Nombre: Ana Carolina Alonso Ramírez
  Tipo y número de documento: CC 52454886
  Correo: aalonso@agenciaatenea.gov.co
- **Rol Supervisión Posmedia:**
  Nombre: Rubith Ofir Tuberquia Avendaño
  Tipo y número de documento: CC 1036599331
  Correo: rtuberquia@agenciaatenea.gov.co

Aún está pendiente la definición del Rol de Supervisión IES para cada institución, y actualmente nos encontramos en proceso de gestión.

Por otro lado, respecto a los textos para documentos y actas dentro del proceso, seguimos en su construcción para su posterior validación jurídica y envío.

Quedo atenta a cualquier requerimiento adicional.

Gracias.

Atentamente,

ANDREA JIMENEZ LOPEZ
Contratista - Procesos
Gerencia Educación Posmedia
Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología – ATENEA
Cra. 10 # 28-49 - Torre A, piso 25. Bogotá D.C. – Colombia

Anexo 3

Número de Control	Control	Estado Control	Evidencia
8.32	Gestión de cambios	En Proceso	Se encuentra en proceso la documentación del procedimiento de gestión de cambios

Anexo 4

Número de Control	Control	Estado Control	Evidencia
8.25	Seguridad en el ciclo de vida del desarrollo	Implementado parcialmente	Se cuenta con un procedimiento formal documentado para el desarrollo de sistemas de información. Se definen fases específicas: análisis, especificación de requisitos, desarrollo, pruebas funcionales y de seguridad, pase controlado a producción, todo bajo ambientes segregados.

Número de Control	Control	Requiere Mejoras	Plan de Acción	RESPONSABLE	Estado Entregables
8.25	Seguridad en el ciclo de vida del desarrollo	Si	Definir una arquitectura general para el desarrollo de aplicaicones-sistemas de información que incorpore el lineamiento de desarrollo seguro		

Anexo 5

Número de Control	Control	Evidencia
8.33	Datos de prueba	Este control se encuentra en proceso de identificación de aplicabilidad de manera técnica en las bases de datos adminsitradas por la Subgerencia TICS

Número de Control	Control	Requiere Mejoras	Plan de Acción	RESPONSABLE	Estado Entregables
8.33	Datos de prueba				

Anexo 6

Número de Control	Control	Evidencia	Requiere Mejoras	Plan de Acción
6.6	Acuerdos de confidencialidad o no divulgación	Los contratos de prestación de servicios incluyen cláusulas de confidencialidad. Para personal de planta y practicantes no contamos con un formato formalmente cargado de acuerdo de confidencialidad firmado individualmente.	Si	Fortalecer la evidencia documental de los compromisos suscritos por funcionarios y practicantes.

Anexo 7

ATENEA	Formato Acta de Reunión	CÓDIGO: F7_P1_DE
		VERSIÓN: 3
	Proceso de Direccionamiento Estratégico	FECHA: 05/05/2023
		Página 2 de 1

TEMA:	Ejecución de las pruebas del plan de recuperación ante desastres para el portal web y la Intranet.
PROCESO:	Gestión de Tecnología de la Información y Comunicación

FECHA:	**2 de diciembre del 2024.**	**Hora Inicio**	**09:00 am**
		Hora Final	**10:00 am**

1. **ORDEN DEL DIA.**

Validación de la ejecución de las pruebas del plan de recuperación ante desastres para los sistemas de información del portal web institucional y la Intranet para el segundo semestre del 2024.

2. **DESARROLLO.**

Se llevó a cabo una reunión con el objetivo de revisar las evidencias de la ejecución y puesta en marcha del plan de recuperación para los sistemas de información indicados. Este proceso contempló la restauración de los servicios tales como networking, seguridad, servidores de aplicación, almacenamientos y bases de datos desde la región primaria a la secundaria. Se ejecutaron las pruebas funcionales sobre las aplicaciones antes y después de ejecutar el plan en ambas regiones. Con este fin, se usaron las herramientas dispuestas en la nube de Oracle para la orquestación y despliegue de los servicios en la región secundaria, así como su replicación de vuelta a la región principal.

La información base para la ejecución de este plan fue proporcionada de manera anticipada por el Ingeniero de Infraestructura y el DBA lo que permitió una revisión ágil y efectiva durante la sesión.

3. **CONCLUSIONES.**

Tras la revisión detallada de la información proporcionada y el análisis de las evidencias entregadas, se concluye lo siguiente:

- Después de revisar las evidencias entregadas, se confirma la correcta ejecución del plan de recuperación ante desastres para los sistemas de información dentro del alcance para el segundo semestre del año 2024.
- Se dio el cumplimiento de los tiempos de RTO, RPO y MTD, para los aplicativos vinculados en la misma.

4. **COMPROMISOS**

No se establecieron compromisos específicos derivados directamente de esta reunión. Teniendo en cuenta las evidencias evaluadas se da por efectuada la prueba a satisfacción.

4.1 PENDIENTES DE REUNIONES ANTERIORES

REUNIÓN	DESCRIPCIÓN	RESPONSABLE	FECHA COMPROMISO	ESTADO
No aplica	No aplica	No aplica	No aplica	No aplica

4.2 PENDIENTES REUNIÓN ACTUAL

REUNIÓN	DESCRIPCIÓN	RESPONSABLE	FECHA COMPROMISO	ESTADO
No aplica	No aplica	No aplica	No aplica	No aplica

5. **LISTADO DE ASISTENCIA**

NOMBRE	FIRMA
Carlos Andrés Ballesteros Castañeda	Firmado digitalmente por CARLOS ANDRES BALLESTEROS
Juan Pablo Ceballos Ospina	
María Alejandra Suarez	Maria Alejandra Suarez Rojas — Firmado digitalmente por Maria Alejandra Suarez Rojas
Edwin Leon Martínez	Firmado digitalmente por Edwin Leon Martinez Motivo: Acta reunion

Anexo 8

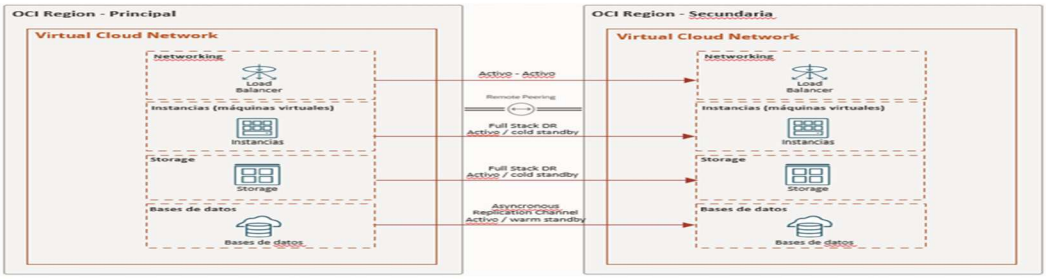
ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE EDUCACIÓN

Seguimiento plan de riesgos relacionados con Disaster Recovery Plan para la infraestructura tecnológica de la entidad.

En la validación de los controles de los riesgos asociados de la dependencia TIC´s, se observó que se tienen definidas las siguientes actividades:

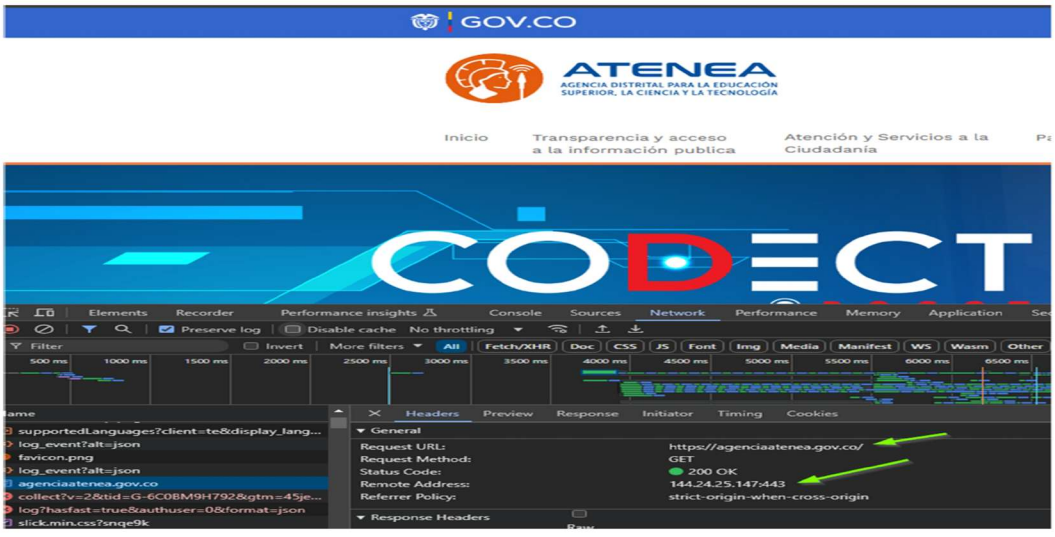
- Realizar un (1) simulacro de recuperación sobre un (1) servicio critico de la Entidad.
- Configurar y puesta en producción del servicio de alta disponibilidad sobre el servicio crítico.
- Restablecer copias de seguridad/imágenes de los servicios tecnológicos que se encuentren afectados.

Se realizó el simulacro de recuperación de la infraestructura que soporta la operación del portal institucional de la entidad (https://agenciaatenea.gov.co). Para esto, se definió la siguiente arquitectura de alta disponibilidad entre la región principal y la secundaria para el portalweb:



- Load balancer: Se tienen configurados Load balancer independientes para cada región con las mismas características y configuraciones, por lo que este elemento hará parte de una estrategia activo-activo.
- Instancias/storage: Transición entre regiones orquestada por el servicio Full Stack Disaster recovery (cold standby).
- Base de datos: Replica a otro MySQL DBsystem en la región secundaria. (activo-activo).

...



Con esta prueba de recuperación se evidenció la correcta ejecución de las replicas/copias de seguridad tomadas a los discos de la aplicación y bases de datos. En esta se contempla no solo la toma de los backups, además se ejecuta una copia de los mismos hacia la región secundaria.

CONCLUSIONES DE LA AUDITORÍA

De acuerdo con el alcance definido en la evaluación de la efectividad del **MSPI - Modelo de Seguridad y Privacidad de la Información**, respecto a los dominios y controles bajo la responsabilidad de la Subgerencia de Tecnologías de Información y Comunicaciones, la Oficina de Control Interno de Gestión concluye que, en líneas generales, el MSPI cumple razonablemente con los requisitos establecidos en la Norma ISO 27001, tanto en su versión 2013 como en la versión 2022.

Para las brechas detectadas, se recomienda reforzar el monitoreo periódico, así como la cultura organizacional en materia de seguridad de la información, e implementar y/o complementar, entre otros, los siguientes mecanismos de control:

- El Oficial de Seguridad de la Información debe reportar directamente a la Alta Dirección o al Comité de Riesgos para asegurar autonomía, evitar conflictos de interés y garantizar decisiones estratégicas y trasversales sobre seguridad de la información de la Agencia.

- Actualizar la Política de Seguridad, incluyendo el manejo de excepciones por incumplimiento y fortalecer los procedimientos de socialización de la política.

- Acelerar la elaboración, formalización e implementación de los procedimientos de borrado seguro, control de cambios, desarrollo seguro y protección de datos de prueba.

- Para mejorar la gestión de accesos, se recomienda: integrar un módulo para administrar usuarios en SICORE; definir una matriz de roles y controles de acceso; revisar y ajustar los perfiles de administrador o soporte en SICORE, SEVEN y KACTUS; actualizar las funciones de los responsables de activos respecto al control de acceso; y formalizar las revisiones periódicas de usuarios en los sistemas de información.

- Establecer un procedimiento formal para realizar, controlar y almacenar las evidencias de pruebas de restauración de respaldos de bases de datos, y ajustar la retención de logs según corresponda.

- Formalizar el uso de acuerdos de confidencialidad individuales, firmados por funcionarios y practicantes que tengan acceso a información institucional sensible.

- Completar el Plan de Recuperación ante Desastres incluyendo la relación de contactos de proveedores y reforzar la documentación técnica y operativa de las pruebas realizadas al DRP.

Para constancia se firma en Bogotá D.C., a los 9 días del mes de octubre del año 2025.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**
Carlos Andrés Ballesteros Castañeda	Subgerente de Tecnologías de la Información y las Comunicaciones	Carlos Ballesteros Firmado digitalmente por Carlos Andres Ballesteros Castañeda
Jorge Luis Garzón Tobar	Jefe Oficina Control Interno de Gestión	JORGE LUIS GARZÓN TOBAR Firmado digitalmente por JORGE LUIS GARZÓN TOBAR Fecha: 2025.10.21 19:28:23 -05'00'
Gloria Janneth Quintero Barandica	Contratista Oficina Control Interno de Gestión	Gloria Janneth Quintero Barandica Firmado digitalmente por Gloria Janneth Quintero Barandica Fecha: 2025.10.22 08:39:20 -05'00'