enterritorio Empresa Nacional Promotora del Desarrollo Territorial S.A.	**INFORME DE SEGUIMIENTO Y EVALUACIÓN (Trabajos de informes, seguimientos de ley y/o cumplimiento)**	CÓDIGO:	**F-AU-10**
		VERSIÓN:	**04**
		VIGENCIA:	**2025-06-12**
	AUDITORÍA INTERNA	CLASIFICACIÓN:	**IP**

N.º 25

EMPRESA NACIONAL PROMOTORA DEL DESARROLLO TERRITORIAL S.A

ASESORIA DE CONTROL INTERNO

Informe de Seguimiento al Modelo de Seguridad y Privacidad de la Información MSPI

PERIODO EVALUADO:
enero 2025 a diciembre 2025

Elaborado:
mayo de 2026

CONTENIDO

LISTA DE TABLAS

LISTA IMAGENES

INFORMACIÓN GENERAL

NOMBRE DEL INFORME:	INFORME DE SEGUIMIENTO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI
TIPO DE INFORME:	Informe de seguimiento
DESTINATARIOS:	Armando Vivas Salamanca - Grupo de Riesgos y Tecnologías de la Información, Carlos Andres Serna Ruiz - Gerente Senior Grupo de Servicios Administrativos y Ciro Antonio Sanchez Pinzon - Gerente Unidad del Grupo de Gestión Talento Humano
FUENTE DE INFORMACIÓN:	Información suministrada por los lideres de SGSI, Subgerencia de operaciones, Talento humano y mesas de trabajo.
EMITIDO POR:	Orlando Correa Nuñez - Asesor con funciones de Control Interno
AUDITOR:	Luz Yanira Salamanca

DESARROLLO DEL INFORME

1. OBJETIVO

Realizar el seguimiento al Modelo de Seguridad y Privacidad de la Información (MSPI), verificando la implementación y aplicación de los controles definidos en la declaración de aplicabilidad.

2. ALCANCE

El seguimiento se efectuó entre enero de 2025 y diciembre de 2025, tomando como referencia una muestra de los controles establecidos en la Declaración de Aplicabilidad F-RI-17 versión 07 (19/09/2025).

3. LIMITACION DEL ALCANCE (SI APLICA)

Para este seguimiento se identificó como limitación la entrega oportuna de la información, dado que se solicitó la información con el radicado 202611010002443 del 05 de mayo de 2026 y se entregó en su totalidad con el radicado 202615010001633 del 28 de mayo de 2026.

4. MARCO LEGAL

- NTC-ISO/IEC 27001:2022 – Anexo A
- M-RI-06 Manual de políticas de seguridad de la información
- O-RI-01 Política Institucional de Seguridad de la Información
- P-RI-19 Gestión de incidentes en seguridad de la información
- P-RI-23 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional

5. RESULTADOS DEL SEGUIMIENTO

5.1. Metodología

El documento F-RI-17 Declaración de Aplicabilidad versión 07 expresa un total de 93 controles implementados, distribuidos de la siguiente manera:

Tabla 1 Controles implementados

Tipo Control	No Controles
A.5 Controles Organizacionales	37
A.6 Controles Personales	8
A.7 Controles Físicos	14
A.8. Controles Tecnológicos	34
Total	**93**

Fuente: Creación propia a partir del documento de declaración de aplicabilidad

Para el seguimiento se seleccionó una muestra de 21 controles, compuesta por:

- ✓ 15 controles no validados en la auditoría MSPI 2024
  - A.5.1 Políticas para la seguridad de la información
  - A.5.7 Inteligencia de amenazas
  - A.5.29 Seguridad de la información durante interrupciones
  - A.5.30 Preparación de las TIC para la continuidad de negocio
  - A.5.32 Derechos de propiedad intelectual
  - A.7.11 Servicios públicos de apoyo
  - A.8.7 Protección contra código malicioso (malware)
  - A.8.9 Gestión de la configuración
  - A.8.10 Eliminación de información
  - A.8.11 Enmascarado de datos
  - A.8.12 Prevención de fuga de datos
  - A.8.16 Actividades de seguimiento
  - A.8.18 Uso de programas de utilidad privilegiados
  - A.8.19 Instalación de software en sistemas operacionales
  - A.8.23 Filtrado web

- ✓ 6 controles seleccionados aleatoriamente
  - A.5.17 Información de autenticación
  - A.5.27 Aprendizaje sobre los incidentes de seguridad de la información
  - A.6.1 Revisión de antecedentes
  - A.6.8 Reportes de eventos de seguridad de la información
  - A.7.7 Escritorio y pantalla limpios
  - A.7.9 Seguridad de activos fuera de las instalaciones

Tabla 2 Controles seleccionados para seguimiento

Tipo Control	Controles Muestra
A.5 Controles Organizacionales	7
A.6 Controles Personales	2
A.7 Controles Físicos	3
A.8. Controles Tecnológicos	9
Total	**21**

Fuente: Creación propia del auditor

5.2. A.5 Controles Organizacionales

A.5.1 Políticas para la seguridad de la información

"Se implementa para establecer lineamientos claros y coherentes que orienten la gestión de la seguridad de la información en toda la organización, garantizando un marco normativo alineado con objetivos estratégicos y requisitos regulatorios."

La entidad dispone del Manual de Políticas de Seguridad de la Información M-RI-06, versión 7 del 28/01/2026, en el cual se definen los objetivos y controles aplicables. Asimismo, la política institucional se encuentra publicada en la página web, dentro del ítem "Nuestra empresa". A través del correo electrónico, se comunicó formalmente al operador tecnológico el manual de políticas, sin embargo, no es remitido a todos los actores externos que también interactúan con la información institucional.

Observación:

Se observaron debilidades en la de comunicación a todos los terceros dado que solo se le comunico al operador tecnológico, el cual que genera riesgos de incumplimiento en la aplicación de lineamientos de seguridad de la información, especialmente en procesos de outsourcing, alianzas o prestación de servicios, afectando la trazabilidad y la responsabilidad compartida en la protección de datos.

A.5.7 Inteligencia de amenazas

"Brinda capacidad de anticipación frente a ciberamenazas, alimentando procesos de gestión de riesgos y mejorando la postura de seguridad."

El control establece que la organización debe contar con capacidades de inteligencia de amenazas que permitan anticiparse a ciberamenazas, alimentando los procesos de gestión de riesgos y fortaleciendo la postura de seguridad, conforme a lo dispuesto en la norma ISO/IEC 27001:2022 – Anexo A.

La entidad ha definido en el numeral 7.5 del Manual de Políticas de Seguridad de la Información M-RI-06 la existencia de un SOC (Security Operation Center), el cual integra los registros de detecciones provenientes de las herramientas de ciberseguridad implementadas.

De acuerdo con la evidencia suministrada por el Oficial de Seguridad, se verificaron los informes de monitoreo SOC correspondientes a los siguientes periodos:

- 27 diciembre 2024 – 26 enero 2025
- 26 marzo – 27 abril 2025

- 27 julio – 26 agosto 2025
- 27 noviembre – 26 diciembre 2025

En dichos informes se observa el monitoreo de eventos críticos, tales como:

- Top 10 *Stealth Scan* o escaneos de descubrimiento
- Top 10 *IPS Attacks* o ataques de red
- Top 10 *IPS Malware/Communications in Devices*
- Top 10 navegación a sitios web maliciosos
- Total de eventos por severidad en casos de uso
- Alertas de alta prioridad
- Verificación de FortiMail, sitios web y casos de *phishing* identificados
- Actividad web y gestión de eventos
- Dispositivos integrados, boletines informativos, conclusiones y recomendaciones

Por lo anterior, al haber implementado un SOC (Security Operation Center) con capacidad de monitoreo continuo y generación de reportes periódicos sobre eventos críticos de ciberseguridad que se encuentran documentados en los informes, demuestra una capacidad efectiva de anticipación frente a ciberamenazas.

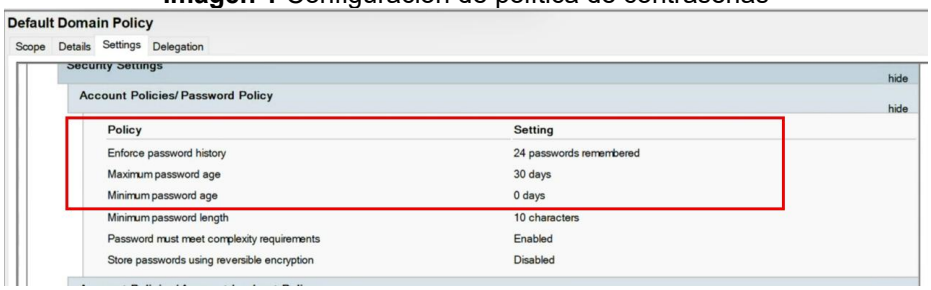
A.5.17 Información de autenticación

"Protege credenciales y mecanismos de autenticación frente a amenazas como robo de contraseñas o phishing."

En la mesa de trabajo realizada el 08 de mayo de 2026 con el operador tecnológico y el oficial de seguridad, se verificó en el Directorio Activo que se encuentra configurada para todos los equipos la política que contempla:

- Cambio obligatorio de contraseña cada 30 días.
- Restricción de reutilización de las últimas 24 contraseñas.

Imagen 1 Configuración de política de contraseñas



Fuente: Imagen tomada durante la reunión.

De acuerdo con el reporte de usuarios en el directorio activo, existen 1.356 cuentas, de las cuales 422 cuentas de contratistas y 57 de planta que tienen activa la opción "password nunca expira" (ver tabla 3). Observación:

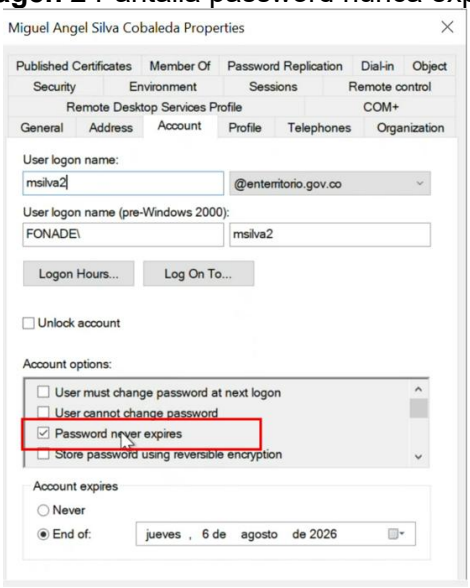
La configuración presentada contraviene la política institucional definida en materia de gestión de contraseñas y afecta la efectividad del control establecido, al incrementar el riesgo de accesos no autorizados y comprometer la robustez del esquema de seguridad.

Tabla 3 Usuarios Activos en el Directorio activo que el password no expira

Descripción	Total Cuentas	Cuentas Activas	Password no expira (Usuarios Activos)	%
Contratista	1.101	779	422	54%
Planta	68	60	57	95%
Otro	187	167	160	96%
Total	**1.356**	**1.006**	**639**	

Fuente: Creación propia del auditor en base del Reporte Usuarios

Imagen 2 Pantalla password nunca expira

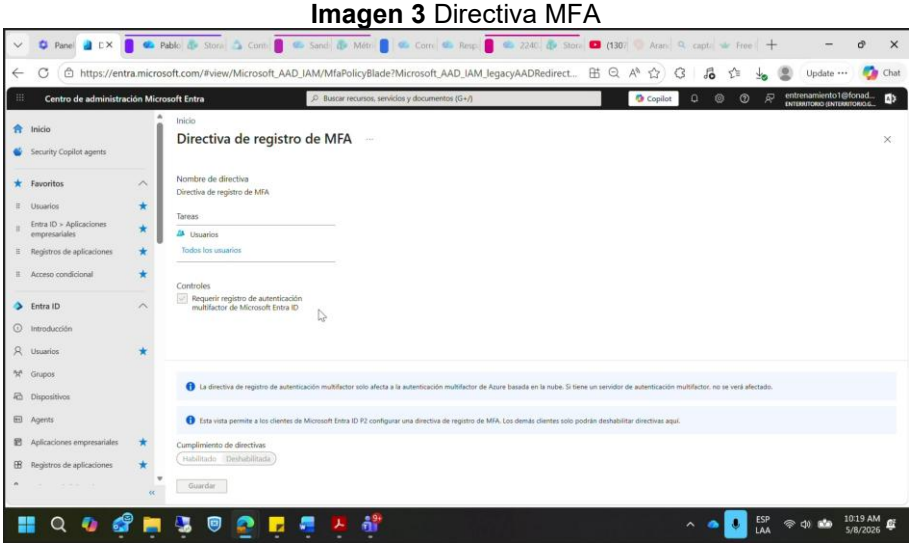


Fuente: Imagen tomada durante la reunión.

La existencia de contraseñas sin fecha de expiración incrementa el riesgo de exposición frente a ataques de fuerza bruta, robo de credenciales o phishing, afectando la robustez del esquema de autenticación y comprometiendo la seguridad de la información institucional.

Por otra parte, se encuentra configurado la directiva de registro MAF mecanismo de seguridad que requiere dos factores de autenticación para validar la identidad de un usuario (doble factor de autenticación).

Imagen 3 Directiva MFA



Fuente: Imagen tomada durante la reunión.

Observación:

De acuerdo con el Manual de Políticas de Seguridad de la Información M-RI-06, numeral 7.15 Información de Autenticación, se establece que *"el cambio de contraseña para los usuarios que tienen configurado este método de autenticación será cada tres (3) meses"*. Sin embargo, durante la verificación se evidenció que esta disposición no se cumple dado que 479 cuentas mantienen activa la *opción "password nunca expira",* lo cual contraviene la política institucional y afecta la efectividad del control.

Así mismo, el manual establece "*Inactivar cuentas de usuario después de treinta (30) días de no uso de las mismas cuando el contrato este vigente.",* sin embargo, en la verificación realizada se evidenció que no existe una política configurada en el Directorio Activo que permita ejecutar automáticamente esta disposición. La ausencia de esta configuración incrementa el riesgo de que cuentas inactivas permanezcan habilitadas en el sistema, lo cual puede ser aprovechado por actores maliciosos para realizar accesos indebidos, comprometiendo la seguridad de la información institucional.

A.5.27 Aprendizaje sobre los incidentes de seguridad de la información
"Facilita la retroalimentación y mejora continua a partir de lecciones aprendidas."

El control establece que la *organización debe facilitar la retroalimentación y la mejora continua a partir de las lecciones aprendidas de los incidentes de seguridad de la información.* Durante el periodo de seguimiento no se registraron incidentes de seguridad de la información en la entidad. En consecuencia, no se generaron informes de lecciones aprendidas ni procesos de retroalimentación derivados de eventos reales.

La entidad cuenta con el Procedimiento de Gestión de Incidentes de Seguridad P-RI-19, en el cual la actividad 11 "I*dentificar lecciones aprendidas*" está claramente definida, asignando como responsables al Oficial de Seguridad de la Información, Oficial de Seguridad Informática y Gerente del Grupo de TI.

Si bien la no ocurrencia de incidentes refleja una adecuada gestión preventiva, la falta de aplicación práctica del proceso de lecciones aprendidas puede reducir la capacidad de la organización para fortalecer sus mecanismos de respuesta y anticiparse a escenarios futuros. Por lo que se recomienda Incorporar referencias de casos externos y buenas prácticas del sector para enriquecer el proceso de retroalimentación y mejora continua.

A.5.29 Seguridad de la información durante interrupciones
"Mantiene la protección de la información aun en situaciones de contingencia o desastre."

A.5.30 Preparación de las TIC para la continuidad de negocio
"Garantiza disponibilidad de los sistemas críticos, soportando el plan de continuidad y recuperación."

Las actividades del Plan de Continuidad del Negocio para la vigencia 2025 se encuentran definidas en el Cronograma del PCN 2025, el cual incluye las pruebas, simulacros y validaciones, junto con sus responsables, periodicidad y ventanas de ejecución el cual se encuentran distribuidas de la siguiente manera:

Tabla 4 Distribución Actividades PNC por trimestre

Actividad Principal	Primer Trimestre	Segundo Trimestre	Tercer Trimestre	Cuarto Trimestre
A. Ejecución Del Plan De Continuidad Del Negocio	6	6	6	3
B. Mantenimiento Y Fortalecimiento De La Estrategia De Continuidad	0	2	2	3
C. Monitoreo Al Plan De Continuidad Del Negocio	3	4	3	5
D. Plan De Sensibilización Y Capacitación	2	6	1	1
E. Plan De Pruebas, Simulacros Y Validaciones	3	5	6	5
Total general	**14**	**23**	**18**	**17**

Fuente: Elaborado ACI a partir del Cronograma del PCN 2025

De acuerdo con el Informe de Plan de Continuidad del Negocio (PCN) del 05 de enero de 2026, se observó el cumplimiento al 100% de las actividades programadas dentro del plan, asegurando la preparación de las TIC para responder ante posibles interrupciones.

Este resultado fue presentado ante el Comité Institucional de Gestión y Desempeño, en la Sesión Ordinaria número 97 del 29 de enero de 2026.

A.5.32 Derechos de propiedad intelectual
"Protege activos intangibles de la organización frente a uso indebido o apropiación no autorizada."

En cuanto al licenciamiento de la Sociedad, el contrato No. 2024612 entre el UT ENTERRITORIO 2027 y ENTERRITORIO S.A con objeto "Prestación de servicios integrales en Tecnologías de Información y

Comunicaciones -TIC, para llevar a cabo la administración, operación, mantenimiento y la gestión de la plataforma tecnológica de ENTerritorio", el cual inició el 27/05/2024 y finaliza el 26/05/2027, describe en los documentos precontractuales y anexos técnicos del proceso INA 007 2024, las obligaciones del operador tecnológico referente al licenciamiento. Los equipos de cómputo y virtualización de servidores para la operación de la Sociedad son bajo la modalidad de arriendo en el marco del contrato 2024612, ANEXO TÉCNICO No. 3 – SERVICIOS DE APROVISIONAMIENTO DE EQUIPOS DE CÓMPUTO Y PERIFÉRICOS.

En la vigencia 2025 se suscribieron los siguientes contratos en relación con el software instalado o de uso en las operaciones de Enterritorio S.A

Tabla 5 Contratos de soporte/mto de software 2025

Nombre del producto	Proveedor	Nro. de Contrato	Fecha de compra	A quiénes se les instaló	Responsable	Vigencia de la licencia	Valor
STATA (Licencias y soporte)	Software Shop de Colombia S.A.S.	2025464	21/02/2025	Grupo de Riesgos	Grupo TI/ Grupo de Riesgos	12 meses	$ 14.458.500
Microsoft Dynamics 365 Finance & Operations (SaaS)	Controles Empresariales S.A.S.	2025563	11/04/2025	Software como servicio para acceso web	Grupo TI	12 meses	$ 1.349.943.036
Microsoft Azure (Suscripción servicios cloud)	Unión Temporal Tigo – Bext 2021	2025570	21/04/2025	Software como servicio para acceso web	Grupo TI	12 meses	$ 444.036.576,61
Oracle Database – Software Update License and Support	Oracle Colombia Ltda.	2025536	29/04/2025	Sistemas de información institucionales	Grupo TI	12 meses	$ 801.743.839
Microsoft Enterprise Agreement (Licenciamiento Microsoft)	Consorcio IAD Dinámico – SoftwareOne	2025602	29/05/2025	Software como servicio para acceso web	Grupo TI	12 meses	$ 1.417.713.540
Adobe Creative Cloud (All Apps)	Panamericana Outsourcing S.A.	2025657	15/07/2025	Usuarios de comunicaciones y diseño	Grupo TI	12 meses	$ 21.000.000
Adobe Acrobat Pro	Panamericana Outsourcing S.A.	2025658	15/07/2025	Usuarios administrativos	Grupo TI	12 meses	$ 27.216.000

Fuente: Tecnologías de la Información

Por lo anterior, se concluye que la Sociedad ha establecido mecanismos contractuales y técnicos para proteger sus activos intangibles frente a uso indebido o apropiación no autorizada. El contrato No. 2024612 suscrito entre UT ENTERRITORIO 2027 y ENTERRITORIO S.A. define de manera explícita las obligaciones del operador tecnológico en materia de licenciamiento, garantizando que los equipos de cómputo y la virtualización de servidores se encuentren bajo la modalidad de arriendo conforme al ANEXO TÉCNICO No. 3. Asimismo, durante la vigencia 2025 se formalizaron contratos adicionales relacionados con el software instalado y utilizado en las operaciones de la entidad, lo que evidencia una gestión alineada con la normativa de propiedad intelectual y la protección de activos intangibles, asegurando la legalidad y trazabilidad de las licencias empleadas en la infraestructura tecnológica.

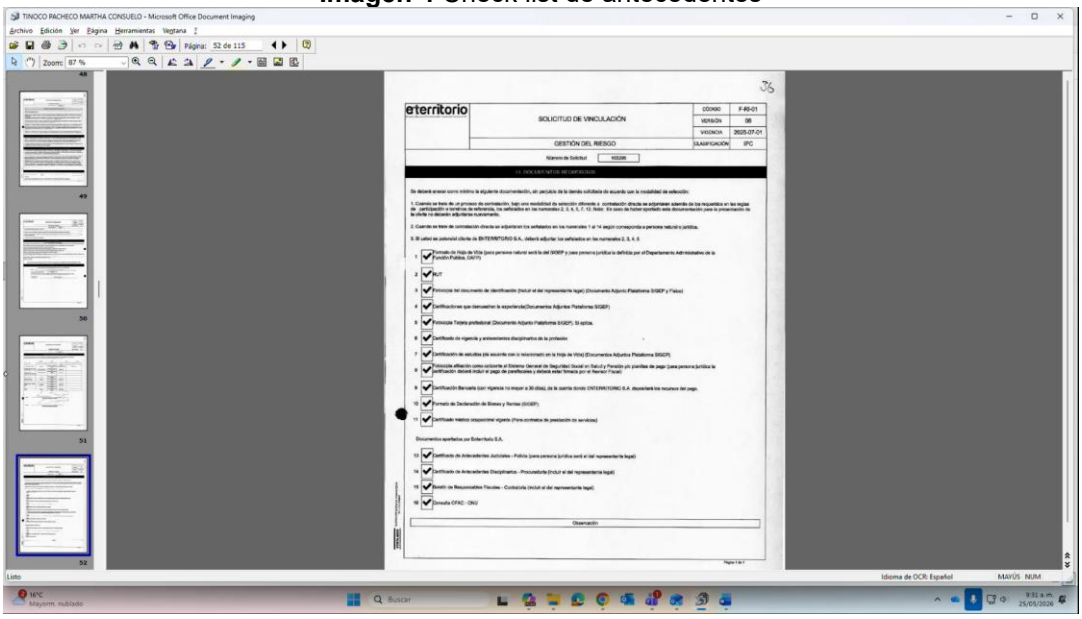
5.3. A.6 Controles Personales

A.6.1 Revisión de antecedentes

"Se implementa para verificar la idoneidad de los candidatos y reducir riesgos de fraude, accesos indebidos o incidentes de seguridad ocasionados por personal con historial incompatible con la función."

Se evidenció que el Procedimiento de Ingreso y Retiro de Personal P-TH-03, versión 8, contempla en la actividad 3 la consulta de antecedentes mediante listas vinculantes, restrictivas y de referencia, lo cual se documenta en el Formato Solicitud de Vinculación F-RI-01 versión 6 del 01 de julio de 2025, ítem 13 "*Documentos requeridos persona natural*". Dichos formatos reposan en la historia laboral almacenada en el SharePoint de Talento Humano.

Imagen 4 Check list de antecedentes



Fuente: Imagen tomada durante la reunión.

Del listado de 55 Trabajadores Oficiales y Empleados Públicos, con corte al 31 de marzo de 2026, se identificó que 22 personas registran fecha de ingreso durante la vigencia 2025. De este grupo se seleccionó una muestra de 10 funcionarios, verificándose en sus historias laborales la existencia del Formato de Solicitud de Vinculación F-RI-01 debidamente firmado, así como el soporte documental de antecedentes correspondiente.

Asimismo, se verificó que en la vigencia 2025, el procedimiento P-TH-03 versión 7 (19 de julio de 2024) no incluía el acuerdo de confidencialidad. Este aspecto fue subsanado en la versión 8 (13 de marzo de 2026), incorporando el Formato F-TH-46 Acta de aceptación y cumplimiento de acuerdo de confidencialidad en la actividad 11. A la fecha, este formato no ha sido utilizado debido a que no se han presentado ingresos de nuevos funcionarios.

A.6.8 Reportes de eventos de seguridad de la información
"*Fomenta la notificación temprana de incidentes o anomalías por parte de empleados y terceros, fortaleciendo la capacidad de respuesta y la gestión proactiva de la seguridad.*"

De acuerdo con el listado de casos registrados en la herramienta Aranda, se evidenció en la vigencia 2025 la notificación de cuatro (4) solicitudes por parte de funcionarios relacionadas con la revisión de correos electrónicos sospechosos. Entre ellas se destacan:

- Solicitudes de confirmación de la confiabilidad del remitente y validación de la apertura de enlaces y/o documentos adjuntos.
- Reporte de un correo con asunto "Su cuenta ha sido hackeada. He robado sus datos", identificado como potencial intento de *phishing* o suplantación.

Estas acciones reflejan la utilización de los canales establecidos para la notificación de anomalías y la activación de la revisión técnica por parte del área de seguridad.

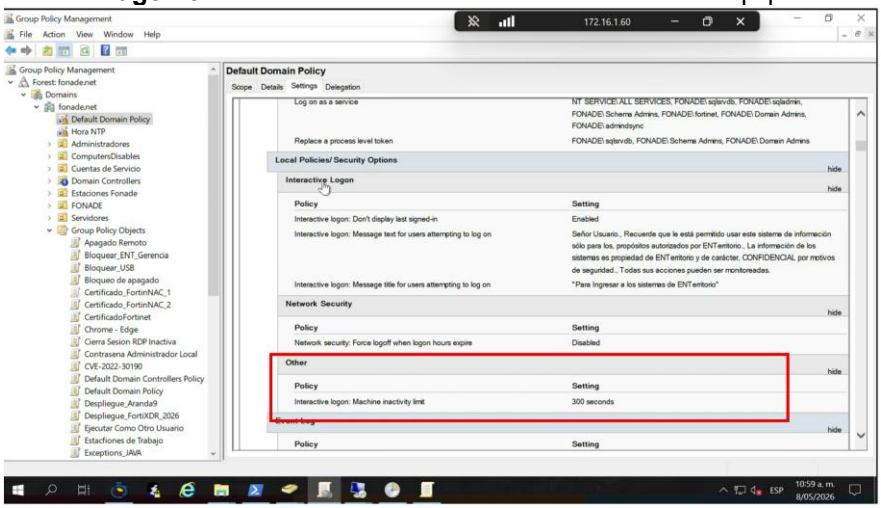
5.3. A.7 Controles Físicos Personales

A.7.7 Escritorio y pantalla limpios
Evita la exposición de información sensible mediante prácticas de orden y seguridad en los puestos de trabajo.

Observación:

De acuerdo con el control CTROPERI-53 Escritorio limpio y pantalla bloqueada – "*El Profesional de Seguridad de la Información y Datos Personales por evento actualiza la política del directorio activo. Esta política se encuentra habilitada para el bloqueo automático de pantalla por inactividad de la estación de trabajo de acuerdo con los intervalos establecidos*". En la mesa de trabajo realizada el 08 de mayo de 2026 se observó la configuración en el Directorio Activo la opción "*Interactive logon: machine inactivity limit*" establecida a 5 minutos (300sg), como se muestra a continuación:

Imagen 5 Directorio activo - Límite de inactividad del equipo



Fuente: Imagen tomada durante la reunión.

El cual no está acorde a lo indicado en el M-RI-06 Manual de políticas de seguridad de la información el numeral 10.1 Dispositivo de punto final de usuario que indica "*Como apoyo para aquellas eventualidades que ocasionan el dejar la estación de trabajo desatendida y sin bloquear, el Grupo de Gestión de las Tecnologías de Información realiza un bloqueo automático de los computadores después de un tiempo de inactividad (4 minutos), pero esta acción debe entenderse como un complemento al deber del colaborador de mantener su estación y su superficie de trabajo bajo su control*."

Se identificó que esta configuración no se encuentra alineada con lo dispuesto en el Manual de Políticas de Seguridad de la Información M-RI-06, numeral 10.1 Dispositivo de punto final de usuario, el cual establece que el bloqueo automático debe realizarse después de 4 minutos de inactividad.

La diferencia entre el tiempo configurado (5 minutos) y el tiempo definido en la política institucional (4 minutos) genera una brecha de cumplimiento que puede incrementar el riesgo de exposición de información sensible en estaciones de trabajo desatendidas.

A.7.9 Seguridad de activos fuera de las instalaciones

"Establece medidas de protección de equipos e información cuando se encuentren en entornos externos, como trabajo móvil o remoto."

De acuerdo con el control asociado CTROPETI-31 "*Control de traslado de componentes de la infraestructura tecnológica dentro y fuera de la Entidad - El Operador Tecnológico por evento autoriza a través de correo electrónico, la salida de equipos asignados en la Sociedad. De igual forma implementa cifrado de disco y protección mediante passaword a la BIOS para equipos portátiles*." se evidencio los correos electrónicos remitidos por parte del Operador Tecnológico a la administración del edificio FONADE, en los cuales se adjuntó el listado de los equipos con salida permanente.

Adicional, como parte de las pruebas de cumplimiento ejecutadas, se efectuó la validación sobre una muestra de doce (12) equipos portátiles, evidenciando que dichos dispositivos cuentan con mecanismos de seguridad implementados, tales como cifrado de disco y protección de acceso a la BIOS mediante

contraseña, controles orientados a salvaguardar la confidencialidad e integridad de la información institucional ante posibles eventos de pérdida, hurto o acceso no autorizado.

A.7.11 Servicios públicos de apoyo
"Garantiza la continuidad de la operación mediante controles sobre electricidad, climatización, telecomunicaciones y otros servicios críticos."

Durante la verificación se constató que la entidad cuenta con 11 Unidades de Potencia Ininterrumpida (UPS) distribuidas de la siguiente manera:

- 10 UPS ubicadas en el edificio CBB de Enterritorio.
- 1 UPS ubicada en el edificio ACH.

En la revisión realizada en los pisos 26, 28 y 29, se observó que las UPS se encuentran en funcionamiento y operando en condiciones normales, garantizando el suministro eléctrico continuo para los sistemas críticos.

Imagen 6 Foto de Operación normal UPS

Fuente: Foto tomada en sitio por el auditor.

Adicional, se evidenció la existencia del Formato F-TI-16 Registro de control de acceso al centro de cómputo y a los cuartos técnicos, en el cual se documenta el ingreso de personal autorizado para la ejecución de mantenimientos preventivos y correctivos. Este registro asegura la trazabilidad de las actividades realizadas en las áreas técnicas y refuerza la seguridad física de la infraestructura.

5.3. A.8 Controles Tecnológicos

A.8.7 Protección contra código malicioso (malware)
Se despliegan soluciones antimalware, listas de bloqueo/permitidos, endurecimiento y concientización para prevenir, detectar y remediar infecciones.

De acuerdo con el control asociado "*CTROPETI-30 Control contra código malicioso El Grupo de Tecnologías de la Información cuenta con una estrategia de limpieza y protección para la prevención de Malware apalancado en el antivirus institucional, la revisión de spam y virus en el correo de la nube del servicio de Office 365, así como las soluciones de seguridad de WAF e IDS las cuales ejecuta por evento sobre la infraestructura tecnológica e información digital de la Sociedad*", se verificó que la entidad utiliza FortiAppSec Cloud, solución de Firewall de Aplicaciones Web (WAF) bajo modalidad SaaS, diseñada

para proteger aplicaciones web y APIs críticas contra ataques comunes como *SQL Injection*, *Cross-Site Scripting (XSS)*, inclusión de archivos maliciosos y accesos no autorizados.
Durante la revisión se constató que:

- En la consola de administración de FortiWeb se identificó que la herramienta tiene configuradas 16 aplicaciones web, cada una con políticas y parámetros de seguridad definidos de acuerdo con las necesidades operativas y requerimientos de protección de los servicios publicados.

- Así mismo, se evidenció que la solución implementa funcionalidades de monitoreo y control sobre el tráfico hacia las aplicaciones expuestas, permitiendo la detección y bloqueo de direcciones IP consideradas potencialmente maliciosas o que presentan comportamientos anómalos. De acuerdo con lo informado por los responsables, previo a la aplicación de bloqueos se realiza el correspondiente análisis y validación de eventos, con el propósito de determinar las acciones a ejecutar y evitar afectaciones sobre la disponibilidad o el acceso legítimo a los servicios institucionales.

- Se evidenció la trazabilidad de los eventos registrados, lo cual permite la gestión proactiva de incidentes y la retroalimentación hacia la administración de riesgos.

Así mismo, la entidad utiliza un Sistema de Detección de Intrusos (IDS) configurado bajo el perfil general denominado “g-SGSI-IPS_ENTERR_General”, el cual permite monitorear el tráfico de red y generar alertas de seguridad en función de la severidad de los eventos detectados.

Durante la verificación se constató que:

- Los eventos clasificados con severidad alta y crítica son bloqueados de manera automática, retroalimentándose con la plataforma FortiWare, lo que asegura una respuesta inmediata frente a intentos de intrusión o ataques relevantes.
- Los eventos de severidad media y baja se mantienen en modo monitor y son remitidos al FortiSIEM, la solución de gestión de información y eventos de seguridad de Fortinet, donde se centraliza y correlaciona la información; posteriormente, estos datos son enviados al Centro de Operaciones de Seguridad (SOC), instancia encargada de realizar el análisis y la validación correspondiente para determinar su relevancia y definir las acciones de respuesta necesarias.

- Se evidenció la trazabilidad de los reportes y la participación del SOC en la gestión de incidentes, lo cual garantiza que las alertas generadas se traduzcan en acciones de control y mejora continua.

A.8.9 Gestión de la configuración

“*Se definen baselines seguras, control de cambios y revisiones periódicas para mantener configuraciones alineadas con buenas prácticas.” A.8.18 Uso de programas de utilidad privilegiados*
”Se controla el uso de utilidades con capacidades elevadas (p.ej., debuggers, escalamiento) mediante listas permitidas y registro de su ejecución.” Y A.8.19 Instalación de software en sistemas operacionales
“Se restringe y autoriza la instalación de software a fin de evitar introducción de riesgos y asegurar licenciamiento.”

De acuerdo con el control asociado "*CTROPERI-46 Restricciones de instalaciones de software. El Grupo de Tecnologías de la Información por evento implementa la política del directorio activo, que restringe la instalación de software por parte de los usuarios finales de los equipos de cómputo de manera automática. El Profesional de Seguridad de la Información y Datos Personales solicita un reporte trimestral sobre los cambios en la línea base de los equipos que están dentro del contrato de arrendamiento*", en la mesa de trabajo realizada el 22 de mayo de 2026, se observó la configuración en el Directorio Activo de la opción "Windows Installer", que bloquea la instalación de software no autorizado.

Se realizo las siguientes pruebas en un portátil obteniendo los siguientes resultados:

- Prueba 1: Se intentó instalar software desde una memoria USB, solicitando credenciales de administrador, lo que confirma la restricción.
- Prueba 2: Se intentó descargar software desde internet, bloqueando la página de instalación.
- Prueba 3: Se probó instalar la aplicación Netflix desde el Microsoft Store con el usuario LSALAMAN; la instalación se completó, pero la aplicación no abrió. Este comportamiento evidencia que, aunque la política limita la instalación de software tradicional, el Store puede ser un vector de incumplimiento si no se controla adecuadamente.

Observación:

Se observaron los informes de los equipos de cómputo, sin embargo, corresponde al seguimiento de los equipos y su respectiva asignación. No se observó los informes de cambio de la línea base de las aplicaciones instaladas de los equipos de cómputo.

En revisión a la matriz de riesgos SIAR, el CTROPERI-46 indica en la columna "ANEXO A ISO 27001:2022" que este asociado al A.8.19 y no se referencia el A.8.9 ni el A.8.18 como se encuentra indicado en la Declaración de Aplicabilidad.

A.8.10 Eliminación de información
"Se dispone la información de forma segura (borrado seguro, destrucción) para evitar divulgación no autorizada al final de su ciclo de vida."

De acuerdo con el control CTROPETI-45 Borrado seguro de datos, se verificó que el Grupo de Tecnologías de la Información, a través del Operador Tecnológico, previo a su entrega, ejecuta un proceso de borrado seguro de la información confidencial.

Durante la revisión documental se observaron 33 actas de certificado de borrado seguro de información, las cuales incluyen:

- Número de placa y serial del equipo.
- Método de borrado utilizado.
- Tiempo de ejecución del proceso.
- Evidencia fotográfica del procedimiento.

Adicionalmente, en la visita en sitio realizada el 12 de mayo de 2026, se constató la ejecución del borrado seguro en el equipo portátil con placa UT0548.

A.8.11 Enmascarado de datos

"Se aplican técnicas de ocultamiento/anonimización en ambientes no productivos o de análisis para proteger datos sensibles y personales."

Durante la vigencia 2025 se evidenció la ausencia de actividades relacionadas con el enmascaramiento de datos en ambientes no productivos, a pesar de que el Manual de Políticas de Seguridad de la Información, en su numeral 10.10, establece de manera expresa que implementa este control como medida de protección de información sensible y personal.

Observación:

Sin embargo, en el Comité Institucional de Gestión y Desempeño #100 – Sesión Ordinaria del 27 de marzo de 2026, se presentó el avance como parte del Plan de Seguridad y Privacidad de la Información – Seguridad Digital la actividad: "*Implementar enmascaramiento de datos de las bases de datos en ambientes de pruebas*", con fecha de inicio 01/04/2026 y fecha de finalización 15/12/2026.
Las tareas definidas incluyen:

- *"Identificar, clasificar y priorizar las bases de datos críticas de la Entidad según sensibilidad, impacto y exposición al riesgo.*
- *Elaborar la ficha técnica de la solución de enmascaramiento de datos.*
- *Evaluar alternativas de mercado y definir la estrategia de implementación bajo un enfoque por fases, priorizando activos críticos y garantizando viabilidad técnica, operativa y presupuestal."*

Se observo el Acta No 1 del 07 de mayo de 2026 cuyo objetivo fue: "Revisar plan de trabajo de enmascaramiento" con el operador UT ENTERRITORIO 2027 y el grupo de gestión de tecnología de información.

En la Declaración de Aplicabilidad F-RI-17_V07, el control A.8.11 se encuentra asociado al control CTROPETI-12 "*Metodología estándar para el desarrollo y/o mantenimiento de aplicativos - Los Grupos de Trabajo y Líderes Funcionales realizan requerimientos a través de la Mesa de Ayuda y aplicativo ARANDA dando cumplimiento al procedimiento Desarrollo, mantenimiento P-TI-04. Una vez evaluadas las necesidades por parte del líder de desarrollo se dará inicio a la solución en caso de ser viable.*" No obstante, este control no contempla de manera expresa el enmascaramiento de datos en ambientes no productivos, lo que genera una brecha normativa y operativa.

La ausencia de actividades de enmascaramiento en 2025 y la falta de inclusión explícita en el procedimiento P-TI-04 reflejan una debilidad en la gestión de datos sensibles en ambientes de pruebas y desarrollo.

A.8.12 Prevención de fuga de datos
"Se implementan controles DLP, cifrado y monitoreo para detectar y bloquear salidas no autorizadas de información."

Durante la validación efectuada sobre una muestra de doce (12) equipos portátiles, se evidenció que dichos dispositivos cuentan con el aplicativo FortiDLP Agent instalado. Este agente forma parte de la solución de Prevención de Pérdida de Datos (Data Loss Prevention – DLP), cuyo objetivo es:

- Monitorear el uso de información sensible en los equipos de cómputo.

- Detectar intentos de copia, transferencia o divulgación no autorizada.
- Aplicar políticas de bloqueo o alerta en caso de incumplimiento.

La instalación del agente DLP en los equipos portátiles reduce significativamente el riesgo de exposición de datos sensibles en ambientes productivos y no productivos.

A.8.16 Actividades de seguimiento

"Se monitorean eventos, alertas y métricas con herramientas de observabilidad/SIEM para detectar y responder a anomalías."

Se verificó que el operador tecnológico realiza informes quincenales de monitoreo sobre las bases de datos institucionales. Dichos informes incluyen:

- Registro de eventos de ingreso a las bases de datos.
- Seguimiento al consumo de espacio y capacidad de almacenamiento.
- Acciones correctivas aplicadas frente a las alertas detectadas.

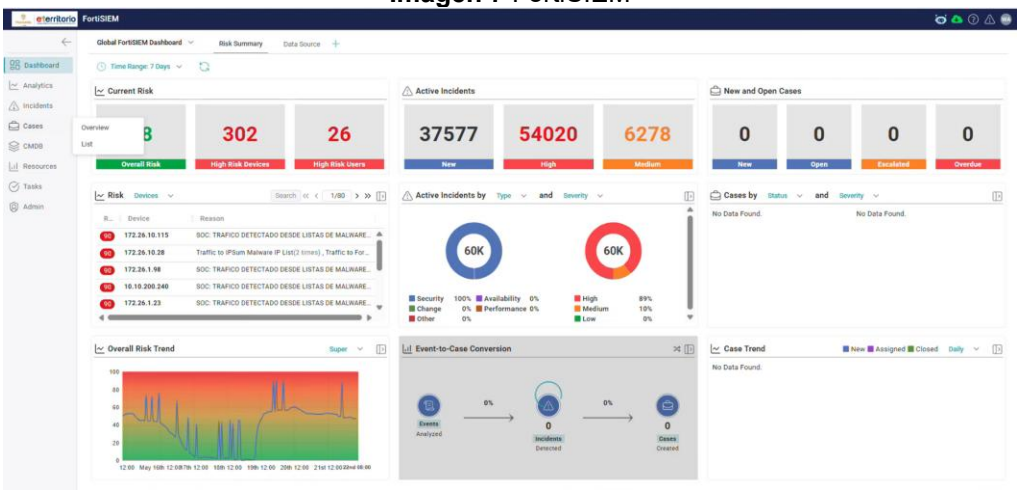
La evidencia documental confirma que los eventos son analizados y que se toman medidas de respuesta en función de las anomalías identificadas, lo cual constituye un mecanismo de seguimiento alineado con el control.

En la mesa de trabajo realizada el 22 de mayo de 2026, se observó el servidor de aplicaciones ENTSRVJBOSS, el cual contiene la aplicación Formulario de Vinculación de Clientes – FVC. Durante la revisión se verificaron los logs generados por el servidor, en los cuales se registran las acciones realizadas por los usuarios y errores presentados en la aplicación. Se guardan los últimos tres meses, sin embargo, queda en el backup de la máquina.

Así mismo, tienen una herramienta Collector que es el encargado de recolectar eventos de múltiples fuentes y enviarlos al FortiSIEM que es una plataforma de SIEM (Security Information and Event Management) desarrollada por Fortinet. Su función principal es centralizar, analizar y correlacionar eventos de seguridad y operación provenientes de múltiples dispositivos y aplicaciones para detectar amenazas, incidentes y problemas de rendimiento. Estos logs se almacenan por un año.

También usan la aplicación ZABBIX que es una plataforma de monitoreo de infraestructura TI, cuya función principal es supervisar el estado, rendimiento y disponibilidad de servidores, redes, aplicaciones, servicios y dispositivos tecnológicos.

Imagen 7 FortiSIEM



Fuente: Imagen tomada en la sesión de trabajo

A.8.23 Filtrado web

"Se controla el acceso a contenidos web mediante listas, categorías y análisis para reducir riesgos de phishing, malware y fuga de datos."

Se verificó que la entidad utiliza FortiAppSec Cloud, solución de Firewall de Aplicaciones Web (WAF) bajo modalidad SaaS, diseñada para proteger aplicaciones web y APIs críticas contra ataques comunes como *SQL Injection*, *Cross-Site Scripting (XSS)*, inclusión de archivos maliciosos y accesos no autorizados.

Durante la revisión se constató que:

- En la consola de administración de FortiAppSec se identificó que la herramienta tiene configuradas 16 aplicaciones web, cada una con políticas y parámetros de seguridad definidos de acuerdo con las necesidades operativas y requerimientos de protección de los servicios publicados.
- Así mismo, se evidenció que la solución implementa funcionalidades de monitoreo y control sobre el tráfico hacia las aplicaciones expuestas, permitiendo la detección y bloqueo de direcciones IP consideradas potencialmente maliciosas o que presentan comportamientos anómalos. De acuerdo con lo informado por los responsables, previo a la aplicación de bloqueos se realiza el correspondiente análisis y validación de eventos, con el propósito de determinar las acciones a ejecutar y evitar afectaciones sobre la disponibilidad o el acceso legítimo a los servicios institucionales.

- Se evidenció la trazabilidad de los eventos registrados, lo cual permite la gestión proactiva de incidentes y la retroalimentación hacia la administración de riesgos.

En revisión a la matriz de riesgos SIAR, el CTROPERI-54 indica en la columna "ANEXO A ISO 27001:2022" que este asociado al A.8.20 y no se referencia al A.8.23

6. CONCLUSIONES

Del total de veintiún (21) controles evaluados en el presente seguimiento, se constató que quince (15) de ellos se encuentran implementados conforme a lo establecido en los controles asociados, no obstante, durante el proceso se identificaron observaciones que reflejan brechas de alineación normativa, limitaciones en la aplicación práctica de ciertos controles y oportunidades de mejora en la trazabilidad y efectividad de las medidas implementadas:

- La entidad dispone de un Manual de Políticas de Seguridad de la Información actualizado (M-RI-06, versión 7 del 28/01/2026) y ha comunicado formalmente la política al operador tecnológico, sin embargo, no se observó la difusión hacia todos los actores externos que interactúan con la información institucional el cual genera una brecha de cumplimiento. Esta limitación incrementa el riesgo de inconsistencias en la aplicación de lineamientos de seguridad, especialmente en procesos de outsourcing, alianzas o prestación de servicios, afectando la trazabilidad y la responsabilidad compartida en la protección de datos.

- En relación al control A.5.17 Información de autenticación, en el Directorio Activo se evidenció la existencia de políticas técnicas orientadas a proteger credenciales, tales como el cambio obligatorio de contraseñas cada 30 días y la restricción de reutilización de las últimas 24 contraseñas. Sin embargo, la efectividad del control se ve debilitada por la configuración de excepciones como la opción “password nunca expira”, el incumplimiento de la directiva que exige el cambio de contraseña cada tres meses según el Manual M-RI-06, y la ausencia de una política automatizada para la inactivación de cuentas de usuario tras 30 días de inactividad.

- El control A.8.11 Enmascarado de datos presenta una brecha en la vigencia 2025, al no haberse realizado actividades de ocultamiento o anonimización de datos en ambientes no productivos, pese a estar definido en el Manual de Políticas de Seguridad. En 2026 se ha iniciado un plan formal con tareas específicas y cronograma, lo que constituye un avance hacia el cumplimiento. En la Declaración de Aplicabilidad F-RI-17_V07, el control A.8.11 se encuentra asociado al control CTROPETI-12 Metodología estándar para el desarrollo y/o mantenimiento de aplicativos, que regula los requerimientos a través de la Mesa de Ayuda y el aplicativo ARANDA, cumpliendo el procedimiento P-TI-04 Desarrollo y mantenimiento. No obstante, este control no contempla de manera expresa el enmascaramiento de datos en ambientes no productivos, lo que genera una brecha normativa y operativa.

- En relación al control A.8.9, A.8.18 y A.8.19, la entidad ha implementado restricciones en el Directorio Activo mediante la opción Windows Installer, lo que impide la instalación de software no autorizado desde medios externos o descargas de internet. Sin embargo, se evidenció que el Microsoft Store permite la instalación de aplicaciones, aunque con limitaciones en su ejecución, lo que representa un vector de incumplimiento si no se controla adecuadamente. Adicionalmente, no se encontraron informes de cambios en la línea base de aplicaciones instaladas en los equipos, lo que genera una brecha en la trazabilidad y seguimiento del control. Finalmente, se identificó una inconsistencia en la matriz de riesgos SIAR, al asociar el control únicamente al A.8.19 y no referenciarlo también al A.8.9 y A.8.18, lo que afecta la correcta alineación como se encuentra indicado en la Declaración de Aplicabilidad.

7. RECOMENDACIONES

- Establecer un mecanismo formal de comunicación y divulgación de las políticas de seguridad de la información hacia todos los actores externos que interactúan con datos institucionales (proveedores, aliados estratégicos, contratistas de outsourcing). Esto permitirá garantizar la trazabilidad, la responsabilidad compartida y la aplicación uniforme de los lineamientos de seguridad en todos los procesos.

- Quitar la configuración que la contraseña nunca expira a los usuarios que están activos. Así mismo, analizar el cambio obligatorio de las contraseñas ya sea cada 30 días o cada 3 meses dado que a todos los colaboradores se les debe habilitar el Doble Factor de Autenticación. Implementar la directiva de inactivación de cuentas tras 30 días de inactividad.

- Ejecutar el plan de enmascaramiento de datos iniciado en 2026, garantizando la inclusión explícita de este control en los procedimientos operativos y normativos. Se recomienda priorizar las bases de datos críticas, definir la ficha técnica de la solución y asegurar la viabilidad técnica y presupuestal para cumplir con lo establecido en el Manual de Políticas de Seguridad.

- Bloquear o restringir el acceso al Microsoft Store para evitar la instalación de aplicaciones no autorizadas, complementando las políticas ya implementadas en el Directorio Activo. Asimismo, la entidad debe generar y mantener informes periódicos sobre los cambios en la línea base de aplicaciones instaladas en los equipos, fortaleciendo la trazabilidad del control.

- Se recomienda alinear la configuración Directorio Activo del bloqueo automático por inactividad el cual se aplica a los (5 minutos) y en el Manual de políticas de Seguridad de M-RI-06 establecido en el (4 minutos)

- Alinear los controles de la matriz de riesgos SIAR y lo definido en la Declaración de Aplicabilidad, asegurando la adecuada referencia de los controles.

Atentamente,

Orlando Correa Núñez
Asesor con Funciones de Control Interno
Elaboró: **Luz Yanira Salamanca – Contratista**

enterritorio
Empresa Nacional Promotora del Desarrollo Territorial S.A.

Al contestar por favor cite estos datos:
Radicado No.: 202611010003493

Pública ☐ **Pública Reservada** ☐ **Pública Clasificada** ☐

MEMORANDO

Bogotá D.C, 10-07-2026 13:51:57

PARA: ESMERALDA MOLINA GOMEZ
Presidenta (e)

ARMANDO VIVAS SALAMANCA
Gerente Grupo de Gestión de Riesgos y TI

CARLOS ANDRES SERNA RUIZ
Gerente Senior Grupo de Servicios Administrativos

CIRO ANTONIO SANCHEZ PINZON
Gerente Unidad del Grupo de Gestión Talento Humano

DE: ORLANDO CORREA NÚÑEZ
Asesor de Control Interno

ASUNTO: Informe definitivo Seguimiento MSPI.

Cordial saludo

Con base en el plan de auditoria aprobado para la vigencia 2026, y posterior al seguimiento realizado, se anexa el informe definitivo establecidas por esta Asesoría.

Así mismo, no se requiere crear un plan de mejoramiento adicional, dado que, las acciones correctivas y preventivas propuestas serán incorporadas al Plan de Acción del SGSI 2026.

Cordialmente,

ORLANDO CORREA NUÑEZ
ASESOR DE CONTROL INTERNO

Proyectó: LUZ YANIRA SALAMANCA - CONTRATISTA - ASESORIA DE CONTROL INTERNO
Elaboró: LUZ YANIRA SALAMANCA - CONTRATISTA - ASESORIA DE CONTROL INTERNO
Adjuntos: 4.5 Informe Definitivo de seguimiento MSPI.pdf(22)

Aprobó: