CORPORACIÓN DE LA INDUSTRIA AERONÁUTICA COLOMBIANA. CIAC S.A.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: PLN-7-00-001
Versión: 10
Fecha de edición: 2 de enero de 2026

AV. Calle 26 No. 103-08 Entrada 1, Interior 2
Bogotá D.C – Colombia

CONTROL DE EMISIÓN

ELABORÓ	REVISÓ	APROBÓ
Nombre: TE. JESSICA TATIANA CIFUENTES DIMAS	Nombre: LUISA CAROLINA SABAS ECHAVARRIA	Nombre: MG. ANDRÉS GUZMÁN MORALES
	Cargo: Vicepresidenta Administrativa	
	Nombre: ALEJANDRA BERNAL WESSO	
	Cargo: Coordinadora SIGCA	
	Nombre: RAFAEL ALBERTO VELASQUEZ GARAVITO	
Cargo: Coordinadora Grupo TICS	Cargo: Jefe Oficina Planeación	Cargo: Presidente

CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	ELABORÓ	FECHA
9	Se actualiza los documentos de referencia, se actualiza el alcance. la situación actual, se incluye la estrategia de seguridad digital, el portafolio de iniciativas y el cronograma de actividades para la vigencia 2025	Profesional Gestión de la Calidad TICS	20 de diciembre de 2025
10	**Actualización de plantilla y contenido:** Adecuación del documento a la nueva plantilla corporativa, ajustando el alcance para la vigencia 2026, los documentos de referencia, los resultados FURAG 2024, las actividades 2025 y la actualización de estrategias, objetivos, metas, portafolio de iniciativas y cronograma de actividades.	Coordinadora Grupo TICS	2 de enero de 2026

TABLA DE CONTENIDO

1 INTRODUCCIÓN

1.1 DOCUMENTOS DE REFERENCIA

1.1.1 Estructura documental SIGCA:

- Plan Estratégico de Tecnologías de la Información (PETI)

1.1.2 Otros documentos de referencia:

- Resolución No. 02277 de 3 de junio de 2025 – “Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”
- Decreto No. 767 de 16 de mayo de 2022 – “Por la cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Resolución No. 500 de 10 de marzo de 2021 - “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- Manual de Gobierno Digital - MINTIC
- Modelo de Seguridad y Privacidad de la Información (MSPI) - MINTIC

1.2 ALCANCE

El Plan de Seguridad y Privacidad de la Información para la vigencia 2026 se enfoca en fortalecer la seguridad digital y la ciberseguridad de la infraestructura tecnológica de la Corporación de la Industria Aeronáutica Colombiana - CIAC, protegiendo la confidencialidad, integridad, disponibilidad y privacidad de los activos de información. Este plan aplica a todos los procesos que gestionen o accedan a la información corporativa.

2 DESARROLLO

2.1 SITUACIÓN ACTUAL

La Corporación de la Industria Aeronáutica Colombiana evalúa el cumplimiento de las políticas de Gobierno Digital y Seguridad Digital por medio del FURAG -Formulario Único Reporte de Avances de la Gestión del Modelo Integrado de Planeación y Gestión de la Función Pública.

Para la vigencia 2024, la Corporación tuvo un puntaje de 95,2 para la Política de Seguridad Digital como se muestra en la siguiente imagen:

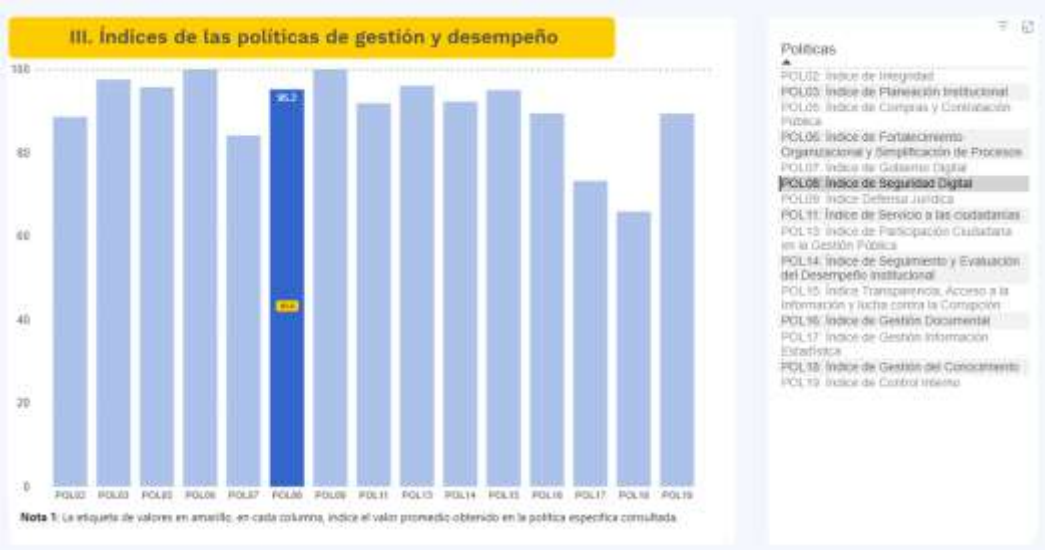

Ilustración 1 Resultado FURAG 2024

Teniendo en cuenta estos resultados se debe mantener lo que se ha implementado y seguir trabajando en el fortalecimiento de esta política.

En la vigencia 2025 para fortalecer y fomentar la seguridad de la información, seguridad digital y ciberseguridad tanto en el entorno laboral como personal, se realizaron las siguientes actividades:

- **Implementación de Network Access Control (NAC):** Se habilitó un control granular de acceso a la red corporativa, permitiendo la conexión exclusiva de dispositivos autorizados. Esta medida reduce significativamente los riesgos asociados a accesos no controlados y refuerza la postura de ciberseguridad corporativa.

- **Implementación del Centro de Operaciones de Seguridad (SOC): Se** puso en marcha un sistema de monitoreo continuo de eventos de seguridad, que permite detectar, analizar y responder de manera oportuna a amenazas cibernéticas, fortaleciendo la capacidad de protección y respuesta ante incidentes.

- **Gestión proactiva de vulnerabilidades:** Se ejecutó la actualización de parches de seguridad en equipos de cómputo y servidores, como parte de una estrategia integral de mantenimiento preventivo y correctivo, orientada a preservar la integridad de la infraestructura tecnológica.

- **Fortalecimiento de la cultura de ciberseguridad:** Se desarrollaron sesiones de inducción y reinducción sobre ciberseguridad, enfocadas en la aplicación de la Política de Seguridad y el Manual de Seguridad y Privacidad de la Información, promoviendo el cumplimiento normativo y la corresponsabilidad institucional.

- **Campañas de sensibilización digital:** Se enviaron comunicaciones periódicas con alertas y recomendaciones de ciberseguridad, orientadas a generar conciencia sobre amenazas emergentes y fomentar buenas prácticas entre los funcionarios.

- **Simulación de ataque de phishing:** Se ejecutó una prueba controlada utilizando Microsoft 365, con el fin de evaluar el nivel de exposición ante ciberataques, identificar vulnerabilidades y fortalecer la capacidad de respuesta individual y colectiva.

- **Primera Semana de la Ciberseguridad:** Se realizó un evento institucional enfocado en sensibilizar a los funcionarios sobre los riesgos digitales, las buenas prácticas y el rol estratégico que cada persona desempeña en la protección de la información corporativa.

2.2 ESTRATEGIA DE SEGURIDAD DIGITAL

La Corporación de la Industria Aeronáutica Colombiana – CIAC, establece una estrategia de seguridad que integra los principios, políticas, procedimientos, manuales y lineamientos para la gestión de la seguridad de la información digital, con base en el Modelo de Seguridad y Privacidad de la Información – MSPI en el marco de la Política de Gobierno Digital.

Teniendo en cuenta lo anterior, la Corporación define las siguientes 5 estrategias que permitirán establecer una estrategia general de seguridad digital, alineadas con el MSPI y la resolución 500 de 2021:

Ilustración 2 Estrategias de Seguridad Digital

2.2.1 Liderazgo De Seguridad De La Información

Asegurar mediante el Manual de Seguridad y Privacidad de la Información (M-7-00-005) y demás lineamientos que se definan, proteger la confidencialidad, integridad y disponibilidad de la información, teniendo como pilar fundamental el compromiso de la Presidencia y de los líderes de las vicepresidencias, oficinas y grupos de la Corporación.

2.2.2 Gestión De Riesgos

Determinar los riesgos de la seguridad de la información digital a través de la planificación y valoración que se defina, buscando prevenir o reducir los efectos indeseados, mediante la implementación de controles de seguridad para el tratamiento de los riesgos.

2.2.3 Implementación De Controles

Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información digital para mantener la confianza en la ejecución de los procesos de la Corporación.

2.2.4 Gestión De Incidentes

Mantener una administración de incidentes de seguridad de la información digital con base en un enfoque de análisis, integración, comunicación de los eventos e incidentes y las debilidades de seguridad digital en pro de detectarlos, evaluarlos y resolverlos para minimizar el impacto negativo que estos puedan ocasionar en la Corporación.

2.2.5 Sensibilización

Fortalecer la cultura organizacional con base en la seguridad de la información digital para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, al igual que reforzar al personal, capacitándole en la necesidad de identificar oportunamente los riesgos de ciberseguridad y adoptar las medidas de seguridad digital necesarias para reducir las posibilidades de pérdida de confidencialidad, integridad y disponibilidad de la información en la Corporación.

Teniendo en cuenta lo anterior, se define las siguientes estrategias de seguridad digital para la vigencia 2026:

Estrategia	Objetivo	Meta
Fortalecer el control de acceso a la red corporativa mediante la actualización, ajuste y monitoreo continuo de los lineamientos de acceso.	Asegurar que el acceso a la red corporativa se realice únicamente desde dispositivos autorizados y que cumplan con los lineamientos corporativos.	Implementar lineamientos de acceso diferenciadas para usuarios internos, externos e invitados en el 100% de la infraestructura de red corporativa.
		Implementar mecanismos de control y monitoreo que permitan identificar y gestionar los intentos

		de conexión no autorizada a la red corporativa.
Consolidar una gestión oportuna y eficiente de los incidentes de seguridad de la información.	Detectar, analizar y responder a los incidentes de ciberseguridad de manera oportuna, con el fin de gestionar su impacto en la operación de la Corporación.	Establecer un tiempo promedio de detección de incidentes de seguridad de la información menor a 1 semana, a través de los mecanismos de monitoreo del SOC.
		Realizar al menos 1 simulacro anual de gestión de incidentes de seguridad de la información durante la vigencia del plan.
Implementar controles técnicos y administrativos orientados a prevenir la pérdida, fuga o uso indebido de la información crítica.	Proteger la confidencialidad de la información corporativa, promoviendo su uso y transmisión de forma segura y conforme a los lineamientos establecidos.	Implementar una solución DLP (Data Loss Prevention) para las herramientas de Microsoft 365 que permita aplicar lineamientos de protección sobre la información crítica.
		Desarrollar actividades de capacitación y sensibilización dirigidas a los funcionarios sobre buenas prácticas para prevenir fugas de información.
Implementar soluciones de cifrado robusto en los equipos portátiles corporativos para proteger la información ante pérdida, robo o acceso no autorizado.	Proteger la confidencialidad e integridad de la información almacenada en los equipos portátiles de la Corporación mediante la aplicación de mecanismos de cifrado.	Implementar el cifrado de disco completo en el 100% de los equipos portátiles corporativos.
		Capacitar al menos al 90% de los usuarios de equipos portátiles en el uso seguro de los dispositivos cifrados.
Fortalecer la cultura de ciberseguridad mediante actividades de sensibilización y simulación de incidentes cibernéticos dirigidos a los usuarios.	Concientizar a los funcionarios sobre los riesgos cibernéticos a los que están expuestos y promover buenas prácticas para la prevención de incidentes de seguridad.	Realizar al menos 3 campañas de sensibilización en ciberseguridad durante la vigencia del plan.
		Implementar un ejercicio controlado de phishing con fines de sensibilización.
		Lograr la participación de al menos el 80% de los funcionarios en las actividades de sensibilización en ciberseguridad.

2.2.6 PORTAFOLIO DE INICIATIVAS

2.2.6.1 Afinamiento Del NAC (Network Access Control)

Esta iniciativa se orienta a fortalecer el control de acceso a la red corporativa mediante el afinamiento de la solución NAC (Network Access Control), la actualización de las reglas de acceso y el fortalecimiento de los mecanismos de autenticación. Su enfoque es asegurar que los dispositivos que se conectan a la red cumplan con los criterios y lineamientos de seguridad definidos por la Corporación.

2.2.6.2 Manejo De Incidentes Mediante El SOC (Security Operations Center)

Esta iniciativa busca consolidar el SOC (Security Operations Center) como el centro de monitoreo para la detección, análisis y gestión de incidentes de seguridad de la información. Incluye la definición y aplicación de protocolos de monitoreo, escalamiento y comunicación de incidentes, con el propósito de mejorar la capacidad de respuesta de la Corporación frente a amenazas internas y externas.

2.2.6.3 Prevención De Fuga De Información (Data Loss Prevention – DLP)

Esta iniciativa se orienta a fortalecer el marco de control para la gestión de la información crítica, mediante la implementación de medidas preventivas y correctivas que abordan los riesgos asociados a la fuga de información, tanto intencional como accidental. Contempla la adopción de tecnologías de prevención de fuga de información (DLP), la definición de lineamientos para la clasificación y manejo de la información, y el fortalecimiento de la cultura organizacional en torno al uso responsable de los datos.

2.2.6.4 Criptografía Para Equipos Portátiles

Esta iniciativa busca proteger la información contenida en los portátiles corporativos mediante la implementación de cifrado de disco completo y lineamientos para la gestión segura de claves. Considerando la movilidad de estos dispositivos y su mayor exposición a riesgos, la criptografía se establece como un control clave para proteger la información frente a accesos no autorizados derivados de pérdida, robo o uso indebido.

2.2.6.5 Sensibilización Sobre Amenazas Y Riesgos Cibernéticos

Esta iniciativa busca fortalecer la cultura organizacional en ciberseguridad, promoviendo el reconocimiento y la gestión de los riesgos mediante campañas de sensibilización y ejercicios controlados de phishing. A través de estas acciones, se impulsa la adopción de buenas prácticas asociadas al factor humano en la seguridad de la información.

2.2.7 CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	RESPONSABLE	FECHA DE INICIO	FECHA FIN	PERIODICIDAD	RESULTADO
Revisar y actualizar los lineamientos y reglas de acceso a la red como parte del afinamiento del NAC	Ingeniero de Infraestructura y Seguridad Informática	2/03/2026 1/06/2026 1/09/2026 1/12/2026	31/03/2026 30/06/2026 30/09/2026 31/12/2026	Trimestral	Lineamientos y reglas actualizadas
Monitorear intentos de conexión no autorizados como	Ingeniero de Infraestructura y Seguridad Informática	1/01/2026	31/12/2026	Mensual	Reporte de intentos bloqueados

parte de la iniciativa de afinamiento del NAC					
Establecer protocolos de respuesta y escalamiento dentro de la iniciativa de manejo de incidentes.	Coordinador TICS Ingeniero de Infraestructura y Seguridad Informática Profesional Gestión de la Calidad TICS	1/07/2026	31/12/2026	Una vez	Documento de procedimientos SOC
Monitorear y detectar incidentes mediante la herramienta SOC.	Ingeniero de Infraestructura y Seguridad Informática	1/01/2026	31/12/2026	Mensual	Reporte de incidentes
Implementar solución DLP en las herramientas de Microsoft 365 como parte de la iniciativa de prevención de fuga de información	Ingeniero de Infraestructura y Seguridad Informática	1/07/2026	31/12/2026	Una vez	Solución implementada
Realizar campañas de sensibilización en fuga de información.	Grupo TICS Grupo CECSA	1/06/2026 1/07/2026	30/06/2026 31/12/2026	Semestral	Formato de capacitaciones LMS y reporte del personal capacitado. O formato de asistencia a la sensibilización
Implementar cifrado de disco en portátiles.	Técnicos de operaciones	2/02/2026	30/06/2026	Una vez	Listado de equipos cifrados
Capacitar a los usuarios de portátiles en uso seguro de dispositivos cifrados.	Grupo TICS	4/05/2026 1/10/2026	29/05/2026 30/10/2026	Semestral	Registro de asistencia
Diseñar e implementar campañas de sensibilización en ciberseguridad.	Grupo TICS Grupo CECSA	2/03/2026 1/06/2026 1/09/2026 1/12/2026	31/03/2026 30/06/2026 30/09/2026 31/12/2026	Trimestral	Formato de capacitaciones LMS y reporte del personal capacitado. O formato de asistencia a la sensibilización
Realizar ataque controlado de phishing	Ingeniero de Infraestructura y Seguridad Informática	2/03/2026	30/06/2026	Anual	Reporte de la simulación

Realizar al menos simulacro de gestión de incidentes.	Ingeniero de Infraestructura y Seguridad Informática	3/08/2026	30/10/2026	Anual	Reporte de la simulación
Revisar y actualizar el Manual de Seguridad y Privacidad de la Información.	Grupo TICS	1/07/2026	31/12/2026	Anual	Documento actualizado
Actualizar parches de seguridad de equipos de cómputo y servidores.	Ingeniero de Infraestructura y Seguridad Informática y Técnicos de operaciones	1/01/2026	31/12/2026	Cada vez que se requiera o mensual	Reporte Desktop Central de parches de seguridad
Ejecutar mantenimientos preventivos y correctivos de los Datacenter y equipos de cómputo.	Ingeniero de Infraestructura y Seguridad Informática y Técnicos de operaciones	6/04/2026	30/05/2026	Anual	Informe de mantenimiento a los data centers y equipos de cómputo mediante y/o informe de recibo a satisfacción.
Validar con los líderes funcionales de SAP que los roles y perfiles asignados correspondan a las funciones que realiza cada usuario.	Profesional Controller SAP y	1/01/2026	31/12/2026	Mensual	Correo enviado al Grupo Comité SAP y el reporte de roles y perfiles.
Verificar que se ejecuten los respaldos de los servidores con la herramienta HERMES y el respaldo en la nube hacía ZEUS.	Ingeniero de Infraestructura y Seguridad Informática y Técnicos de operaciones	1/01/2026	31/12/2026	Mensual	Informe enviado por el proveedor
Verificar que se ejecuten de manera automática las copias de respaldo de las máquinas virtuales.	Ingeniero de Infraestructura y Seguridad Informática y Técnicos de operaciones	1/01/2026	31/12/2026	Mensual	Correos que envía de manera automática la herramienta de backup

3 ANEXOS

No aplica