PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., /2025

TABLA DE CONTENIDO

1. OBJETO 3
2. DOCUMENTOS DE REFERENCIA 3
3. JUSTIFICACIÓN 3
4. ALCANCE 4
5. RESPONSABLE 4
6. DEFINICIONES 4
7. DESARROLLO 5
7.1 SITUACIÓN ACTUAL 5
7.2 ESTRATEGIA DE SEGURIDAD DIGITAL 8
7.2.1 Liderazgo De Seguridad De La Información 8
7.2.2 Gestión de Riesgos 9
7.2.3 Implementación de Controles 9
7.2.4 Gestión de Incidentes 9
7.2.5 Sensibilización 9
7.3 PORTAFOLIO DE INICIATIVAS 10
7.3.1 Control de Acceso a la Red (NAC) 11
7.3.2 Administración de Acceso Privilegiado (PAM) 11
7.4 CRONOGRAMA DE ACTIVIDADES 11

LISTA DE ILUSTRACIONES

Ilustración 1 Resultados FURAG 2023 6
Ilustración 2 Resultados Simulación Microsoft 365 7
Ilustración 3 Estrategias de Seguridad Digital 8

1. OBJETO

Establecer la estrategia de seguridad digital y ciberseguridad para fortalecer la disponibilidad, integridad y confidencialidad de los activos de información en la Corporación de la Industria Aeronáutica Colombiana - CIAC.

2. DOCUMENTOS DE REFERENCIA

- 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"
- Resolución No. 1519 de 24 de agosto de 2020 - "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos."
- Manual de Gobierno Digital - MINTIC
- Modelo de Seguridad y Privacidad de la Información (MSPI) - MINTIC
- POL-1-01-009 – Política de Seguridad de la Información
- M-7-00-005 – Manual de Seguridad y Privacidad de la Información

3. JUSTIFICACIÓN

Es necesario establecer la estrategia de seguridad digital para fortalecer la disponibilidad, integridad y confidencialidad de los activos de información de la CIAC, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y la Comunicaciones – MinTIC y las disposiciones legales que apliquen en cuanto a seguridad digital y ciberseguridad.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información se enfoca en la seguridad digital y la ciberseguridad de la infraestructura tecnológica evitando que se vea afecta la confidencialidad, integridad y disponibilidad de los activos de información en la Corporación de la Industria Aeronáutica Colombiana - CIAC.

5. RESPONSABLE

Coordinador Grupo TIC'S

6. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Activos de Información y Recursos: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016)

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Ciberdelincuente: Persona que busca sacar beneficio de los problemas o fallos de seguridad encontrados en programas, servicios, plataformas o herramientas, utilizando distintas técnicas como la ingeniería social o el malware (https://www.incibe.es/aprendeciberseguridad/)

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados. (Resolución 7870 de 2022)

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a personas, entidades o procesos autorizados. (ISO/IEC 27000)

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera (ISO/IEC 27000)

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos (ISO/IEC 27000)

Seguridad de la Información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000)

Seguridad Digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales. (Modelo de Seguridad y Privacidad de la Información - MinTIC)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas (ISO/IEC 27000)

7. DESARROLLO

7.1 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 2023, la Corporación tuvo un puntaje de 87,6 para la Política de Seguridad Digital como se muestra en la siguiente imagen:

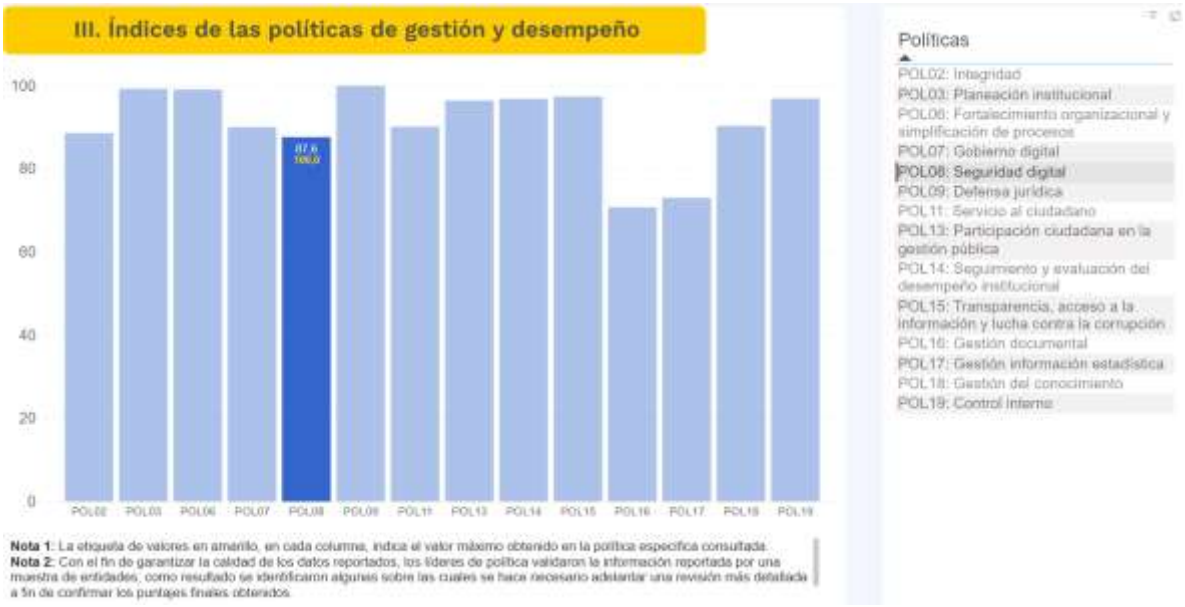

Ilustración 1 Resultados FURAG 2023

Teniendo en cuenta estos resultados se debe seguir trabajando en la implementación y el fortalecimiento de esta política.

En la vigencia 2024 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:

- Activación del doble factor de autenticación para el ingreso del correo electrónico
- Actualización Manual de Seguridad y Privacidad de la Información (M-7-00-005), ajustando políticas como: Política de uso del correo electrónico corporativo, Política de uso de los sistemas o herramientas tecnológicas y política de respaldo y recuperación.
- Actualización de parches de seguridad de los equipos de cómputo y los servidores
- Sesiones de sensibilización a todo el personal sobre ciberseguridad, las cuales se realizaron con la ayuda del proveedor de Fortinet y CSIRT MinDefensa.
- Implementación ADSelf Service, solución de seguridad de identidad que permite la gestión de contraseñas seguras evitando la utilización de palabras genéricas como “Ciac2024”, “Agosto2024” “123456789”, información personal como la identificación o fechas.

- Charlas de inducción y reinducción al personal sobre ciberseguridad y la aplicación de la Política de Seguridad y el Manual de Seguridad y Privacidad de la Información.
- Envío de correos con alertas de seguridad cibernética y recomendaciones de ciberseguridad.
- Capacitaciones mediante SuccessFactors sobre ciberseguridad y uso de herramientas TI como SharePoint.
- Realización de simulación de ataque de phishing utilizando Microsoft 365. A continuación, vemos los resultados.

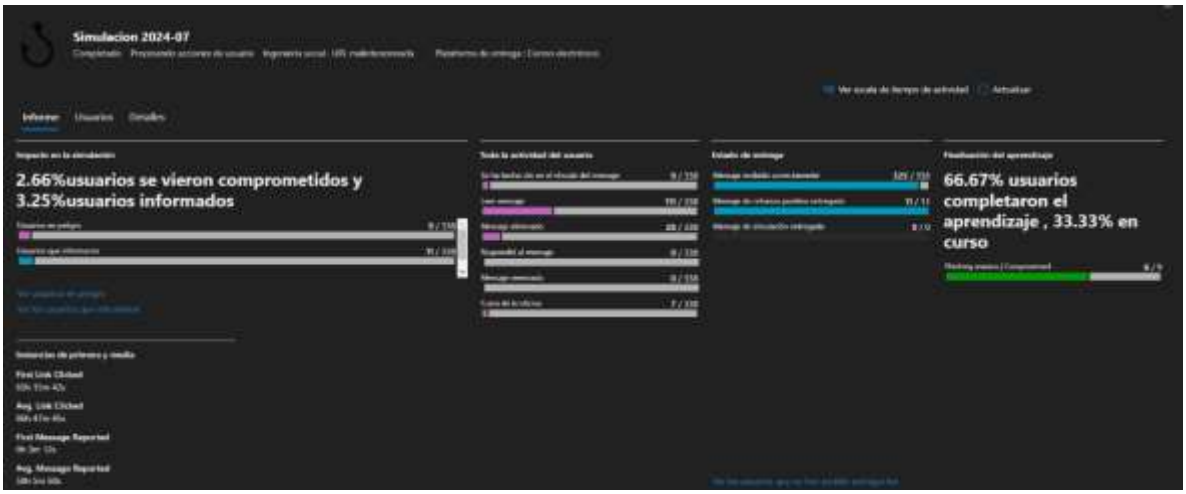

Ilustración 2 Resultados Simulación Microsoft 365

Los datos que arrojó la simulación son los siguientes:

Simulación Phishing Julio 2024	
Acciones del Usuario	**Cantidad**
Correos enviados	338
Clic en el vínculo del mensaje	9
Leer mensaje	111
Mensaje eliminado	28
Respondió el mensaje	0
Mensaje reenviado	0
Completaron el aprendizaje	6

La misma herramienta envió a los usuarios comprometidos en la prueba, una capacitación de refuerzo para minimizar los riesgos a los cuales pueden estar expuestos y evitar ser víctimas de los ciberdelincuentes.

7.2 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 3 Estrategias de Seguridad Digital

7.2.1 Liderazgo De Seguridad De La Información

Asegurar mediante la Política de Seguridad de la Información (POL-1-01-009), 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, departamentos y gerencias de la Corporación.

7.2.2 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.

7.2.3 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.

7.2.4 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.

7.2.5 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 realiza el siguiente resumen con la estrategia de seguridad digital para la vigencia 2025:

Estrategia	Objetivo	Meta
Liderazgo de Seguridad de la Información	Definir lineamientos para proteger la confidencialidad, integridad y disponibilidad de la información	Revisar y actualizar la documentación
Gestión de Riesgos	Determinar y gestionar los riesgos asociados a los activos de	Identificación activos de información críticos

	información críticos para el funcionamiento de la Corporación	Identificar, evaluar y gestionar los riesgos asociados a los activos de información críticos
Implementación de Controles	Implementar controles para mitigar los riesgos identificados	Restringir el acceso de usuarios y dispositivos no autorizados a la red (Control de Acceso a la Red (NAC))
		Proteger las cuentas privilegiadas (Administración de Acceso Privilegiado (PAM))
		Corregir fallos de seguridad que puedan ser explotados por atacantes
		Prolongar la vida útil de los equipos y asegurar el rendimiento de los equipos y en los Datacenter
		Asegurar que los colaboradores tengan acceso a los roles y perfiles de SAP necesarios para realizar su trabajo de manera efectiva.
		Verificar la realización de los backups de los servidores y las copias de respaldo de las máquinas virtuales
Gestión de Incidentes	Minimizar el impacto de los incidentes de seguridad digital	Monitorear los eventos e incidentes y las debilidades de seguridad digital para minimizar el impacto negativo que estos puedan ocasionar
		Simular ataques cibernéticos dirigidos a los usuarios para evaluar su reacción ante estos incidentes.
Sensibilización	Fortalecer la cultura organizacional con base en la seguridad de la información digital	Fortalecer la cultura organizacional para que todos se sientan responsables de la protección de la información.
		Mantener a los usuarios actualizados sobre las últimas tendencias y tácticas de ataque, permitiéndoles adaptarse y defenderse mejor.

7.3 PORTAFOLIO DE INICIATIVAS

Se contemplan las siguientes iniciativas relacionadas con la gestión de seguridad y privacidad de la información y alineados con el Plan Estratégico de Tecnologías de la Información – PETI.

7.3.1 Control de Acceso a la Red (NAC)

Con esta iniciativa se pretende hacer un acceso de confianza cero, supervisando y protegiendo los activos digitales conectados a la red corporativa, cubriendo dispositivos TI, permitiendo visibilidad, control y respuesta automatizada para todo aquello que se conecta a la red. Esta iniciativa está dentro de la estrategia de implementación de controles y está alineada con la estrategia del fortalecimiento de la ciberseguridad y el objetivo de fortalecer la ciberseguridad para proteger la información digital establecidos en el PETI y se contempla dentro del proyecto de fortalecimiento de la gestión TI

7.3.2 Administración de Acceso Privilegiado (PAM)

Con esta iniciativa se pretende asignar niveles de permiso más altos a cuentas con acceso a recursos críticos y controles a nivel administrativo, basándose en el principio de privilegio mínimo, como mejor práctica de ciberseguridad. Esta iniciativa está dentro de la estrategia de implementación de controles y está alineada con la estrategia del fortalecimiento de la ciberseguridad y el objetivo de fortalecer la ciberseguridad para proteger la información digital establecidos en el PETI y se contempla dentro del proyecto de fortalecimiento de la gestión TI

7.4 CRONOGRAMA DE ACTIVIDADES

Se realizarán las siguientes actividades para dar cumplimiento a las estrategias establecidas de seguridad digital en la vigencia 2025:

No.	Estrategia	Actividad	Evidencia	Ejecución	Responsable
1	Liderazgo de Seguridad de la Información	Revisar y actualizar la política de Seguridad de la Información	Documento actualizado	31/12/2025	Coordinador TICS y Profesional de Gestión de la Calidad TICS
2	Liderazgo de Seguridad de la Información	Revisar y actualizar el Manual de Seguridad y Privacidad de la Información	Documento actualizado	31/12/2025	Equipo TICS
3	Gestión de Riesgos	Identificar activos de información críticos para el funcionamiento de la Corporación	Actas de mesas de trabajo y/o formato de asistencia	31/12/2025	Equipo TICS

4	Gestión de Riesgos	Identificar, evaluar y gestionar los riesgos asociados a los activos de información críticos para el funcionamiento de la Corporación	Matriz de riesgos	31/12/2025	Equipo TICS
5	Implementación de Controles	Seguimiento a la iniciativa control de acceso a la red (NAC)	Ejecución y documentación del proyecto	29/08/2025	Coordinador TICS y Profesional de Infraestructura
6	Implementación de Controles	Seguimiento a la iniciativa administración de acción de acceso privilegiado (PAM)	Ejecución y documentación del proyecto	29/08/2025	Coordinador TICS y Profesional de Infraestructura
7	Implementación de Controles	Actualizar parches de seguridad de equipos de cómputo y servidores	Reporte Desktop Central de parches de seguridad	Mensualmente	Profesional de Infraestructura y Técnico de operaciones
8	Implementación de Controles	Ejecutar mantenimientos preventivos y correctivos de los Datacenter y equipos de cómputo	Informe de mantenimiento a los data centers y equipos de cómputo mediante y/o informe de recibo a satisfacción.	31/12/2025	Técnico de operaciones y Profesional de Infraestructura
9	Implementación de Controles	Validar con los líderes funcionales de SAP que los roles y perfiles asignados correspondan a las funciones que realiza cada usuario.	Correo enviado al Grupo Comité SAP y el reporte de roles y perfiles.	Mensualmente	Profesional Controller SAP
10	Implementación de Controles	Verificar que se realicen los backups de los servidores con la herramienta HERMES y el respaldo en la nube hacía ZEUS	Informe enviado por el proveedor	Mensualmente	Técnico de operaciones y Profesional de Infraestructura
11	Implementación de Controles	Verificar que se ejecuten de manera automática las copias de respaldo de las máquinas virtuales	Correos que envía de manera automática la herramienta de backup	Mensualmente	Técnico de operaciones y Profesional de Infraestructura

12	Gestión de Incidentes	Actualizar indicador de disponibilidad	Reporte de indicadores	1/04/2025 1/07/2025 1/10/2025 31/12/2025	Profesional de Gestión de la Calidad TICS
13	Gestión de Incidentes	Simular ataques de phishing	Reporte de la simulación	27/06/2025 31/12/2025	Profesional de Infraestructura
14	Sensibilización	Enviar correos con alertas de seguridad cibernética y/o recomendaciones de ciberseguridad	Correos de las alertas y/o recomendaciones	31/03/2025 27/06/2025 30/09/2025 31/12/2025	Equipo TICS
15	Sensibilización	Realizar inducciones y/o reinducciones al personal sobre temas de ciberseguridad y seguridad digital	Presentación de inducción o formato de asistencia a inducción personalizada	27/06/2025 31/12/2025	Profesional de Infraestructura
16	Sensibilización	Educar y sensibilizar a los usuarios sobre amenazas y riesgos cibernéticos a los que pueden estar expuestos.	Formato de capacitaciones LMS y reporte del personal capacitado. O formato de asistencia a la sensibilización	31/03/2025 27/06/2025 30/09/2025 31/12/2025	Coordinador TICS y Profesional de Gestión de la Calidad TICS