PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., /2023

1. OBJETO

Establecer la estrategia y acciones para mantener y mejorar la seguridad y privacidad de la información y seguridad digital, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información en la Corporación de la Industria Aeronáutica Colombiana - CIAC.

2. DOCUMENTOS DE REFERENCIA

- Gobierno Digital
- Modelo de Seguridad y Privacidad de la Información – MSPI
- Estándar Internacional de Seguridad BASC 5.0.1
- Norma ISO IEC 27001:2013
- Resolución No. 001519 de 24 de agosto de 2020
- Conpes 3975 – Política Nacional para la Transformación Digital e Inteligencia Artificial del 8 de noviembre de 2019
- Conpes 3854 - Política Nacional de Seguridad Digital de Colombia del 11 de abril de 2016

3. JUSTIFICACIÓN

Es necesario determinar la estrategia y las acciones que se deben tomar para mantener y mejorar la seguridad y privacidad de la información en la CIAC, teniendo en cuenta la implementación del 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 cubre las actividades establecidas para mantener y mejorar la seguridad y privacidad de la información y seguridad digital, basado en los lineamientos del Modelo de Seguridad y Privacidad de la Información establecido por MinTIC.

5. RESPONSABLE

Coordinador Gestión TIC's

6. DEFINICIONES

Activo de Información: Es todo aquello que tiene valor para la Corporación y que, por lo tanto, requiere de protección.

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

Ciberseguridad: conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la Corporación en el Ciberespacio. (Glosario mintic.gov.co)

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.

7. SITUACIÓN ACTUAL

En la vigencia 2022 se actualizó la Política Global de Seguridad y Privacidad de la Información (POL-1-01-009), al igual que el Manual de Seguridad y Privacidad de la Información (M-7-00-005), documentos publicados en el sitio web corporativo en el enlace de transparencia y en Isolución.

El Manual de Seguridad y Privacidad de la Información tiene como objetivo establecer las políticas y lineamientos de seguridad de la información en la Corporación de la Industria Aeronáutica Colombiana, con el fin de mantener la confidencialidad, integridad y disponibilidad de la información dando cumplimiento al Modelo de Seguridad y Privacidad de la Información – MSPI de Gobierno Digital.

Debido a las constantes amenazas informáticas es necesario realizar un diagnóstico de seguridad de la información, con el fin de determinar las acciones para el tratamiento de nuevos riesgos en materia de seguridad y privacidad de la información, mediante el fortalecimiento e implementación de políticas y lineamientos, al igual que crear y actualizar la documentación referente a la seguridad y privacidad de la información en la CIAC.

7.1 NIVEL DE RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Oficina de Planeación, Innovación y Desarrollo realiza sesiones de trabajo con todos los procesos para actualizar y verificar la matriz de riesgos que incluyan en ellas los aspectos relacionados con el riesgo de la seguridad y privacidad de la información a nivel tecnológico. Cada proceso debe determinar los niveles de riesgos y los controles para mitigar los mismos.

7.2 ANÁLISIS DE VULNERABILIDADES

Gestión TIC's con el equipo de infraestructura revisa mensualmente los informes generados por los aliados de seguridad informática de las herramientas de Sophos, Fortinent y Antivirus Kaspersky, para identificar los eventos de seguridad que

puedan poner en riesgo la seguridad de la información o la infraestructura tecnológica. En caso de e encontrarse amenazas y vulnerabilidades, se agenda una reunión con los proveedores para afinar la herramienta si requiere o se toman las medidas correspondientes para corregir las amenazas y vulnerabilidades encontradas.

Así mismo, se cuenta con la herramienta de seguridad de Office 365 que mediante inteligencia artificial con el Antivirus Kaspersky cada vez que se genere una novedad de intento de envío o recibo de algún tipo de spam y/o correo malicioso, el sistema envía a cuarentena la posible amenaza para ser gestionados con base en el análisis de la información realizado por el Coordinador de Gestión TICS y/o técnico de infraestructura. Adicionalmente, se implementó en el correo corporativo la funcionalidad para que el usuario pueda reportar la suplantación de identidad cuando considere que se trata de un correo de tipo phishing.

Estas medidas permiten controlar las amenazas y vulnerabilidades que se puedan presentar en la Corporación, aunque siempre hay que estar alerta ya que día a día aparecen nuevas amenazas y vulnerabilidades.

7.3 SENSIBILIZACIÓN

La principal línea de defensa en materia de seguridad y privacidad de la información es el usuario, una cadena es tan fuerte como el más débil de sus eslabones, es por esa razón que se trabaja constantemente en reforzar al personal, capacitándole en la necesidad de identificar oportunamente los riesgos de ciberseguridad y adoptar las medidas de seguridad de la información necesarias para reducir las posibilidades de pérdida de confidencialidad, integridad y disponibilidad de la información de la Corporación.

Buscando mejorar el nivel de conciencia de cada colaborador de la Corporación, se realizan charlas de inducción y reinducción al personal sobre ciberseguridad y la aplicación del Manual de Seguridad y Privacidad de la Información. De igual manera, en la vigencia 2022 se han establecido capacitaciones mediante SuccessFactors para que el personal pueda minimizar los riesgos a los cuales puede estar expuesto y evitar ser víctima de los ciberdelincuentes.

7.4 PROGRAMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para mantener y mejorar la seguridad y privacidad de la información, preservando la confidencialidad, integridad y disponibilidad de la información en la CIAC, se establecen las siguientes actividades para la vigencia 2023:

No.	ACTIVIDAD	RESPONSABLE	EVIDENCIA	FECHA DE EJECUCIÓN
1	Analizar los reportes mensuales de las plataformas de seguridad informática (Fortinet, Sophos y Kaspersky)	Coordinador GTIC's y grupo de infraestructura	Informes de seguridad reportados por los proveedores mensualmente y F-7-00-003 - formato de control de cambios	Del 10 de febrero al 20 de diciembre de 2023
2	Realizar campañas trimestrales de sensibilización sobre temas de ciberseguridad	Profesional Gestión de la Calidad TIC's y grupo de infraestructura	Presentación de inducción y/o formato de capacitaciones LMS y reporte del personal capacitado y/o correos de las campañas realizadas sobre ciberseguridad.	1. Del 16 de enero al 31 de marzo de 2022 2. Del 3 de abril al 30de junio de 2022 3. Del 4 de julio al 29 de septiembre de 2022 4. Del 2 de octubre al 22 de diciembre de 2022
3	Realizar pruebas semestrales de vulnerabilidades	Técnico de Infraestructura	Informe resultado pruebas de vulnerabilidad	Del 16 de enero al 30 de junio y del 4 de julio al 15 de diciembre de 2023
4	Actualizar inventario de Software y Hardware para identificar los activos asociados con la información	Técnico de Operaciones	Formato de inventario actualizado	Cada vez que se requiera o el último día hábil de cada mes. Del 30 de enero al 30 de diciembre de 2023

5	Realizar soporte y mantenimiento del ERP SAP, con el fin de mantener la seguridad, confidencialidad e integridad del sistema de información.	Coordinadora SAP y Controller SAP	Reporte de ticket's de la mesa de ayuda y la herramienta SAP Solution Manager	Del 30 de enero al 30 de diciembre de 2023
6	Actualizar parches de seguridad equipos de cómputo	Técnico de Operaciones	Reporte Desktop Central de parches de seguridad	Del 30 de enero al 29 de diciembre de 2023
7	Actualizar parches de seguridad servidores	Técnico de Infraestructura	Reporte Desktop Central de parches de seguridad	Del 30 de enero al 29 de diciembre de 2023
8	Ejecución de mantenimientos preventivos y correctivos de los Datacenter y equipos de cómputo	Equipo de Infraestructura	Informe de mantenimiento a los data centers y equipos de cómputo mediante y/o informe de recibo a satisfacción.	30 de noviembre de 2023
9	Actualización del I-7-00-010 Instructivo de gestión de incidentes informáticos para la seguridad de la información	Profesional Gestión de la Calidad TIC's y equipo de infraestructura	Instructivo actualizado y publicado en Isolución	15 de diciembre de 2023
10	Actualización del plan de recuperación de desastres tecnológicos o el plan de continuidad tecnológico.	Profesional Gestión de la Calidad TIC's y equipo de infraestructura	Plan actualizado y publicado en Isolución	15 de diciembre de 2023