PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., /2024

1. OBJETO

Establecer la estrategia y acciones para mantener y mejorar la seguridad y privacidad de la información 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

- Norma Internacional BASC V6:2022
- Estándar Internacional de Seguridad BASC 6.0.1
- Norma ISO IEC 27001:2013
- Gobierno Digital
- Modelo de Seguridad y Privacidad de la Información – MSPI
- 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
- 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.”
- 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 determinar la estrategia y las acciones que se deben tomar para mantener y mejorar la seguridad y privacidad de la información digital 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 se enfoca en la protección de la infraestructura tecnológica para evitar vulnerabilidades que afecten la confidencialidad, integridad y disponibilidad de la seguridad de la información digital.

5. RESPONSABLE

Coordinador Gestión 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. SITUACIÓN ACTUAL

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 la plataforma de 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, teniendo en cuenta:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

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, Fortinet 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 esto 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, debido a esto, en la vigencia 2023 se enviaron correos con alertas de seguridad cibernética, recomendaciones de ciberseguridad y capacitaciones mediante SuccessFactors para que el personal minimice los riesgos a los cuales puede estar expuesto y evitar ser víctima de los ciberdelincuentes.

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 de la Política de Seguridad y el Manual de Seguridad y Privacidad de la Información.

Para la vigencia 2024 se continuará con el envío de correos informativos, campañas de sensibilización, charlas de inducción y reinducción al personal en temas de ciberseguridad, seguridad digital y las políticas de seguridad de la información para generar conciencia entre los colaboradores sobre los actuales y potenciales riesgos que podrían afectar los activos de información, la información institucional y personal, así como los lineamientos y directrices que se deben seguir.

7.4 PROGRAMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Programa de Seguridad y Privacidad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información digital, mediante las siguientes actividades para la vigencia 2024:

No.	ACTIVIDAD	RESPONSABLE	EJECUCIÓN	EVIDENCIA
1	Analizar los reportes de las plataformas de seguridad informática y ejecutar las recomendaciones que sean pertinentes. (Fortinet, Sophos y Kaspersky)	Coordinador GTIC's y grupo de infraestructura	Mensual	Informes de seguridad reportados por los proveedores mensualmente
2	Realizar campañas de sensibilización sobre temas de ciberseguridad	Coordinador GTIC's, Profesional Gestión de la Calidad TIC's y	Cada vez que se presente una alerta o trimestralmente	Presentación de inducción y/o formato de capacitaciones LMS y reporte del personal

		grupo de infraestructura		capacitado y/o correos de las campañas realizadas sobre ciberseguridad.
3	Realizar pruebas de vulnerabilidades	Técnico de Infraestructura	Semestralmente	Informe resultado pruebas de vulnerabilidad
4	Actualizar inventario de Software y Hardware para identificar los activos asociados con la información	Técnico de Operaciones	Cada vez que se requiera o el último día hábil de cada mes.	Formato de inventario actualizado
5	Realizar soporte y mantenimiento del ERP SAP, con el fin de mantener la seguridad, confidencialidad e integridad del sistema de información.	Controller SAP	Diariamente	Reporte de ticket's de la mesa de ayuda y la herramienta SAP Solution Manager
6	Actualizar parches de seguridad equipos de cómputo	Técnico de Operaciones	Cada vez que se requiera	Reporte Desktop Central de parches de seguridad
7	Actualizar parches de seguridad servidores	Técnico de Infraestructura	Cada vez que se requiera	Reporte Desktop Central de parches de seguridad
8	Ejecución de mantenimientos preventivos y correctivos de los Datacenter y equipos de cómputo	Equipo de Infraestructura	Anualmente	Informe de mantenimiento a los data centers y equipos de cómputo mediante y/o informe de recibo a satisfacción.
9	Actualizar el instructivo de VeamBackup	Profesional Gestión de la Calidad TIC's y equipo de infraestructura	Cada vez que se requiera o una vez en el año	Instructivo actualizado y publicado en Isolución
	Actualizar el procedimiento de monitoreo de servidores	Profesional Gestión de la Calidad TIC's y equipo de infraestructura	Cada vez que se requiera o una vez en el año	Procedimiento actualizado y publicado en Isolución

10	Actualizar el plan de recuperación de desastres tecnológicos.	Profesional Gestión de la Calidad TIC's y equipo de infraestructura	Cada vez que se requiera o una vez en el año	Plan actualizado y publicado en Isolución
11	Validar con los líderes funcionales de SAP que los roles y perfiles asignados correspondan a las funciones que realiza cada usuario.	Profesional Controller SAP	Cada vez que se requiera o los primeros 10 días de cada mes	Correo enviado al Grupo Comité SAP y el reporte de roles y perfiles.
12	Verificar que se realicen los backups de los servidores con la herramienta HERMES y el respaldo en la nube hacía ZEUS	Equipo de Infraestructura	Semanalmente	Informe enviado por el proveedor
13	Verificar que se ejecuten de manera automática las copias de respaldo de las máquinas virtuales	Equipo de Infraestructura	Diariamente	Correos que envía de manera automática la herramienta de backup
14	Brindar soporte sobre los recursos o servicios TI (sitio web, red, correo electrónico, hardware, software y/o infraestructura de red)	Equipo de Infraestructura	Diariamente	Ticket's de la mesa de ayuda