PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., /2023

1. OBJETO

Identificar y gestionar los riesgos de seguridad y privacidad de la información y seguridad digital, con el fin con el fin de proteger 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
- Guía para administración del riesgo y el diseño de controles en entidades públicas Vr. 5
- Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas
- Manual Del Sistema Integral De Gestión De Riesgos – M-1-03-003

3. JUSTIFICACIÓN

Es necesario gestionar y controlar los riesgos de seguridad y privacidad de la información y seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información en la Corporación.

4. ALCANCE

El Plan de Tratamiento de Riesgos Seguridad y Privacidad de la Información aplica para todos los activos de información de la CIAC, y aborda las etapas de

identificación y gestión del riesgo de seguridad y privacidad de la información y seguridad digital, teniendo en cuenta la metodología establecida en la Corporación para la gestión de riesgos.

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.

Amenaza: Son las acciones que aprovechan vulnerabilidades para romper la seguridad de los sistemas.

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)

Impacto: Las consecuencias que puede ocasionar a la Entidad la materialización del riesgo

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

Riesgo Inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: Nivel resultante del riesgo después de aplicar los controles.

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.

Vulnerabilidad: Una vulnerabilidad es un fallo técnico o deficiencia de un programa que puede permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

7. GESTIÓN DE RIESGOS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la gestión de riesgos en seguridad y privacidad de la información y seguridad digital se toma como referencia la metodología definida para la elaboración de los Mapas de Riesgos establecida en el M-1-03-003 Manual del Sistema Integral de Gestión de Riesgos CIAC.

Para la identificación de riesgos de seguridad de la información, es necesario identificar los activos de la información, teniendo en cuenta los siguientes pasos:

1. Listar los activos por cada proceso
2. Identificar el dueño de los activos
3. Clasificar los activos
4. Clasificar la información
5. Determinar la criticidad del activo
6. Identificar si existe infraestructura crítica cibernética

Se identificarán los siguientes tres (3) riesgos inherentes de seguridad digital:

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

Así mismo, se debe analizar las posibles amenazas y vulnerabilidades que podrían causar la materialización de cada riesgo.

Se debe tener en cuenta que la sola presencia de una vulnerabilidad no causa daños por sí misma, debido a que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

A continuación, se muestra ejemplos de vulnerabilidades y amenazas, de acuerdo con el tipo de activo.

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Tomado de la Guía paras la administración del riesgo y el diseño de controles en entidades públicas Vr. 5

7.1 Roles y Responsabilidades

7.1.1 Coordinador GTIC´s

- Identificar, analizar, evaluar y controlar los riesgos que afecten la seguridad y privacidad de la información y seguridad digital realizando su actualización anualmente.
- Aplicar la metodología de gestión de riesgos establecida y realizar el posible cambio de controles.
- Conocer los mapas de riesgos inherentes y residuales confirmando que estos corresponden a la situación real de la Corporación.
- Garantizar la correcta aplicación de los controles asociados para el tratamiento de los riesgos inherentes.
- Implementar las oportunidades de mejora que se identifiquen en las actividades de monitoreo continuo (Autocontrol, Autorregulación, Autogestión), y las actividades de monitoreo independiente realizadas por la Oficina de Control Interno.
- Comunicar la metodología de gestión de riesgos y de los controles.
- Reportar trimestralmente la materialización de riesgos a la Oficina de Planeación, Innovación y Desarrollo para su seguimiento y cierre. Confirmar, en caso de que no exista ningún reporte, la ausencia de este.

7.1.2 Colaboradores GTIC’S

- Los colaboradores del grupo de Gestión TIC’s, mantendrá su rol acorde a las funciones desempeñadas aplicando cada uno de los controles diseñados en la matriz de riesgos.
- Los administradores responsables de la infraestructura mantienen actualizada las vulnerabilidades de los sistemas operativos de cada uno de los servidores acorde a las publicaciones del fabricante.
- Conocer y aplicar las políticas de seguridad de la información, establecidas en el Manual de Seguridad y Privacidad de la Información.
- Mantener informado al Coordinador TIC’S, sobre cualquier anomalía o posible ataque en la que se vea en inminente riesgo la infraestructura informática o la información.
- El acceso a las tecnologías de la Corporación será expresamente aprobado por el coordinador y el personal responsable de dicha herramienta debe estar

preparado para atender la solicitud y mantener el control en la seguridad informática.

- Cuando se requiera que un tercero o partner acceda a la información o la infraestructura informática interna, copien, modifiquen, o procesen la información, se debe exigir, que se establezcan las medidas adecuadas para la protección de la información de acuerdo con su clasificación y análisis de riesgo contempladas en los acuerdos de confidencialidad y/o contractualmente se tengan claros estos ítems bajo la supervisión del funcionario de la Corporación.

7.2 VALORACIÓN DEL RIESGO

Una vez identificados los riesgos de seguridad digital con sus respectivas amenazas y vulnerabilidades, se continua con la valoración del riesgo que contempla las actividades de identificación, análisis y evaluación de riesgos, las cuales se detallan en el Manual del Sistema Integral de Gestión de Riesgos – M-1-03-003.

7.3 IDENTIFICACIÓN Y EVALUACIÓN DE LOS CONTROLES EXISTENTES

Una vez identificados y valorados los riesgos inherentes, se debe identificar y evaluar los controles existentes, los cuales se toman como referencia el Anexo A de la Norma ISO IEC 27001:2013, como insumo base para mitigar los riesgos de seguridad digital, siempre y cuando se ajusten al análisis de riesgos.

7.4 TRATAMIENTO DEL RIESGO

Una vez identificados los riesgos, se define el tratamiento para cada uno de los riesgos analizados y evaluados, que involucra la selección de una o más actividades de control para disminuir sus consecuencias (impacto) o la frecuencia y así establecer si el nivel de riesgo residual (después de controles) se encuentra dentro de los niveles de aceptación por parte de la Corporación.

La evaluación de los controles se realiza teniendo en cuenta los siguientes criterios:

- Por lo adecuado de las actividades y suficiencia del control.
- Por su oportunidad
- Por su naturaleza
- Por su periodicidad

- Por su Funcionalidad
- Por su evidencia

Cada criterio se detalla en el Manual del Sistema Integral de Gestión de Riesgos – M-1-03-003

7.5 ACTIVIDADES DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para identificar y gestionar los riesgos de seguridad y privacidad de la información y seguridad digital, con el fin con el fin de proteger la confidencialidad, integridad y disponibilidad de la información en la Corporación de la Industria Aeronáutica Colombiana - CIAC., se establecen las siguientes actividades para la vigencia 2023:

No.	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Identificar los riesgos de seguridad y privacidad de la información y seguridad digital, teniendo en cuenta los activos de la información.	Coordinador GTIC's y profesional Gestión de la Calidad TIC's	30 de junio de 2023
2	Clasificar los riesgos de seguridad y privacidad de la información y seguridad digital	Profesional Gestión de la Calidad TIC's y grupo de infraestructura	30 de agosto de 2023
3	Evaluar los riesgos de seguridad y privacidad de la información y seguridad digital	Profesional Gestión de la Calidad TIC's y grupo de infraestructura	29 de septiembre de 2023
4	Identificación y evaluación de los controles existentes	Profesional Gestión de la Calidad TIC's y grupo de infraestructura	31 de octubre de 2023
5	Tratar los riesgos de seguridad y privacidad de la información y seguridad digital	Profesional Gestión de la Calidad TIC's y grupo de infraestructura	30 de noviembre de 2023