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

Bogotá D.C., /2024

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
- Norma ISO IEC 27001
- Norma Internacional BASC
- Estándar Internacional de Seguridad BASC
- 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. 6
- 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

Se requiere 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, dando cumplimiento al Modelo de Seguridad y Privacidad de la Información de MINTIC, la política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y la normatividad establecida.

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

Oficina de Planeación, Innovación y Desarrollo

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).

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)

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. (Modelo de Seguridad y Privacidad de la Información - MinTIC)

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 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

7.1 ESTABLECIMIENTO DEL CONTEXTO

En el contexto se relacionan los aspectos internos y externos que se deben tener cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información y

Seguridad Digital de la CIAC. A partir de este contexto es posible determinar las posibles causas de los riesgos a identificar.

7.2 IDENTIFICACIÓN DEL RIESGO

La identificación de los riegos busca una relación de los posibles puntos de peligro, lo que se identifique será analizado, lo que no quedará como riesgo oculto o ignorado.

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

A nivel de seguridad de la información se identifica los siguientes tres (3) tipos riesgos:

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

Así mismo, se debe analizar las posibles amenazas y vulnerabilidades que podrían causar la materialización de cada riesgo, ocasionando pérdidas o alteración en el funcionamiento de la Corporación o poniendo en riesgo el cumplimiento de los objetivos corporativos.

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. 6

7.3 VALORACIÓN DEL RIESGO

Previo a la valoración del riesgo de seguridad de la información y seguridad digital, se debe contar con el inventario de activos de información d ellos procesos, que es la base para la valoración de los riesgos.

La valoración es la determinación del costo que supondría recuperarse de una incidencia que dañe el activo. La valoración puede ser cuantitativa o cualitativa.

La valoración se puede ver desde la perspectiva de la necesidad de proteger, pues cuanto más valioso es un activo, mayor nivel de protección requiere para que no se vea afectada su confidencialidad, integridad o su disponibilidad, según sea pertinente.

7.4 IDENTIFICACIÓN Y EVALUACIÓN DE LOS CONTROLES EXISTENTES

Una vez identificados y valorados los riesgos, 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 y seguridad de la información, siempre y cuando se ajusten al análisis de riesgos.

7.5 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 y que no se vea afectada la disponibilidad, integridad y confidencialidad de la información.

Para el tratamiento del riesgo se debe tomar alguna de las siguientes opciones:

- **Aceptar el riesgo:** Cuando se reconoce la existencia del riesgo y sus consecuencias (provisión de las posibles pérdidas), sin necesidad de tomar otras medidas de control diferentes a las que poseen. Algunos riesgos serán aceptados excepcionalmente mediante la aprobación del dueño del proceso, siempre y cuando el riesgo esté ubicado de acuerdo con el apetito de riesgo de la Corporación. Se debe realizar un seguimiento continuo del riesgo.
- **Evitar el riesgo:** Se evita el riesgo si se decide no proceder con la actividad que probablemente generaría el riesgo, utilizando un activo, servicio o producto distinto o modificando el proceso, de manera que las amenazas originales ya no lo afecten.
- **Transferir el riesgo:** Esto involucra que un externo a la entidad soporte o comparta el riesgo. Los mecanismos pueden incluir el uso de contratos, arreglos de seguros y estructuras organizacionales tales como sociedades entre otros.
- **Reducir o mitigar el riesgo:** Actividades y medidas tendientes a reducir la probabilidad y/o minimizar la severidad de su impacto. Se consigue mediante la optimización de los procedimientos y la implementación de controles (prevención, planificación).

7.6 MATERIALIZACIÓN

En el caso de materializarse un riesgo se debe seguir el Instructivo Gestión de Incidentes de Seguridad de la Información (I-7-00-022), y se deberá analizar el riesgo y realizar la respectiva valoración posterior a la materialización, dejando el registro en el mapa de riegos. Cuando se materialice un riesgo que no se haya identificado, deberá ser reportado e iniciar el respectivo procedimiento de valoración del riesgo.

7.7 ACTIVIDADES

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	Ejecución	Fecha Inicio	Fecha Fin
1	Revisar los lineamientos de riesgos para seguridad y privacidad de la información y seguridad digital	Anual o cada vez que se materialice un riesgo	1/03/2024	31/05/2024
2	Identificar y/o actualizar los activos de información	Anual o cada vez que se materialice un riesgo	1/03/2024	31/12/2024
3	Valorar y priorizar los riesgos de seguridad y privacidad de la información y seguridad digital.	Anual o cada vez que se materialice un riesgo	2/05/2024	31/12/2024
4	Identificar y evaluar los controles existentes	Anual o cada vez que se materialice un riesgo	2/07/2024	31/12/2024