PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., /2022

1. OBJETIVO

Establecer la estrategia y acciones necesarias para mantener y mejorar el sistema de seguridad y privacidad de la información.

2. JUSTIFICACIÓN

En el desarrollo de la era digital y de las tecnologías de la información y las comunicaciones, donde se ha transformado la forma de acceder a la información, el desarrollo del negocio, el consumo de tecnologías, y la aplicabilidad de los sistemas de información es necesario actualizar periódicamente el diagnostico de seguridad de la información de la CIAC determinando las acciones necesarias para los documentos que lo componen requiriendo cada vez, ser más competitivos.

3. ALCANCE

El plan de seguridad y privacidad de la información cubre los aspectos para mantener y mejorar las políticas de seguridad de la información, el programa de seguridad de la información, plan de recuperación de desastres tecnológicos para la Corporación de la Industria Aeronáutica Colombiana.

4. RESPONSABLE

Coordinador Grupo de Gestión de Tecnologías de la Información.

5. DEFINICIONES

Activo de información. Cualquier componente (humano, tecnológico, SOFTWARE, documental o de infraestructura) que soporta uno o más procesos de negocios de la Corporación y, en consecuencia, debe ser protegido.

Acuerdo de confidencialidad (NDA). Es un documento en el que los colaboradores de la CIAC S.A. o de terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Corporación, comprometiéndose a no divulgar, usar o explotar la información a la que tengan acceso en virtud de la labor desarrollada dentro o en relación con la misma por cualquier medio utilizado.

Análisis de riesgos de seguridad de la información. Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de tales variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

BACKUP (Copia de seguridad). Copia de seguridad de uno o más archivos informáticos, que se hace, generalmente, para prevenir posibles pérdidas de información.

Planeación de capacidades. Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la Corporación a fin de satisfacer las necesidades de procesamiento de tales recursos de forma eficiente y con un rendimiento adecuado.

Centro de cableado. Es un sitio destinado para la instalación de dispositivos de comunicación y cableado. Debe cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo. Es una zona determinada para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. Debe cumplir estándares tendientes a garantizar controles de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones medioambientales adecuadas.

Ciberseguridad. La ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término es amplio y se aplica a numerosos elementos, desde seguridad informática hasta recuperación ante desastres y educación del usuario final. (según ksp, https://latam.kaspersky.com)

Cifrado. Es la transformación de datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) ante posible interceptación y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad. Es la garantía de que la información no estará disponible o será divulgada a personas, entidades o procesos no autorizados.

Control. Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía. Es la disciplina que agrupa los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio y/o prevenir su uso no autorizado.

Custodio del activo de información. Es la unidad organizacional o proceso, designado por la organización para mantener las medidas de protección necesarias sobre los activos de información confiados.

Derechos de autor. Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad. Es la garantía de acceso a la información y a los activos asociados cuando los usuarios así lo requieren en todo tiempo y momento.

Equipo de cómputo. Es el Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Guías de clasificación de la información. Son las directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con ello, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

HACKING ético. Es el conjunto de actividades para ingresar a las redes de datos y voz institucionales con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intención maliciosa, ni delictiva y sin generar daños en los sistemas o redes, que se realizan con el propósito de mostrar el nivel efectivo de riesgo al cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de seguridad. Es un evento adverso, confirmado o bajo sospecha, que ha vulnerado la seguridad de la información o que intenta vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias o el origen (interno o externo).

Integridad. Es la protección de la exactitud y estado completo de los activos de información.

Inventario de activos de información. Es una lista ordenada y documentada de los activos de información pertenecientes a la Corporación.

Licencia de SOFTWARE. Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un producto de SOFTWARE, definiendo los alcances de uso, instalación, reproducción y copia.

Medio removible. Es cualquier componente extraíble de HARDWARE usado para el almacenamiento de información. Incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario. Son características específicas y especiales de cada usuario que permiten privilegios de acceso y uso a los recursos tecnológicos o los sistemas de información de acuerdo con las funciones realizadas en la Corporación.

PRDT: plan de recuperación de desastres tecnológicos.

Propiedad intelectual. Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información. Es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos. Son aquellos componentes de HARDWARE y SOFTWARE tales como servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos

de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros; los cuales tienen como finalidad apoyar las tareas administrativas y logísticas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Corporación.

Registros de auditoría. Son archivos que contienen eventos identificados en los sistemas de información, recursos tecnológicos y redes de datos de la Corporación, los cuales pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas dentro o fuera de la CIAC S.A. tales como intentos de acceso exitosos y/o fallidos, cambios en la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información. Es la persona o grupo de personas designadas por la Corporación encargados de velar por la confidencialidad, integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger los activos a su cargo.

SGSI. Sistema de Gestión de Seguridad de la Información.

Sistema de información. Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información requiriendo a su vez de la interacción de uno o más activos de información para efectuar las tareas previstas. Puede ser de origen interno o de origen externo conforme a las necesidades de la Corporación.

Sistemas de control ambiental. Son sistemas que utilizan un proceso de tratamiento del aire permitiendo modificar ciertas características del mismo, tales como humedad y temperatura, con el fin de asegurar un ambiente controlado de trabajo para los equipos ubicados dentro de un área específica.

SOFTWARE malicioso. Programa malicioso o MALWARE que contiene virus, SPYWARE u otros programas indeseados con el objeto de infiltrarse, secuestrar o dañar los recursos tecnológicos, los sistemas operativos, las redes de datos o los sistemas de información.

Terceros. Todas las personas, jurídicas o naturales, tales como proveedores, contratistas o consultores, que provean servicios o productos a la Corporación.

Vulnerabilidades. Son puntos débiles, huecos en la seguridad o flaquezas en los activos de información que pueden ser explotadas por factores externos y/o internos, no controlables por la Corporación, los cuales se constituyen en fuentes de riesgo.

6. DIAGNÓSTICO DE SITUACIÓN EN SEGURIDAD

Debido a los constantes cambios en las amenazas informáticas es necesario actualizar periódicamente el diagnóstico de seguridad de la información (Instrumento de evaluación MSPI 2018) de la Corporación con el fin determinar con precisión las acciones para el tratamiento de nuevos riesgos en materia de seguridad de la información.

Las acciones determinadas dentro de este plan están:

6.1. Nivel de riesgo en seguridad y privacidad de la información institucional

Se realizan sesiones de trabajo liderada por la oficina de Planeación, Innovación y Desarrollo con todos los procesos de la Corporación 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. Plan que se encuentra publicado dentro de la documentación de Gestión de la Calidad de la Corporación y que el dueño del proceso debe tener en cuenta para poder determinar los niveles de riesgos y los planes que debe adoptar en cada uno de los procedimientos a su cargo junto con los colaboradores de cada dependencia.

6.2 Análisis de Vulnerabilidades

El grupo de GTIC´s, interesado en este tema de ataques informáticos que contempla ciberataques y cibercriminalidad para la Corporación, solicita a través de los entes de control aliados con las herramientas que se vienen desarrollando con el Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa y Policía Nacional como es el Comando Conjunto de Operaciones Cibernéticas CCOC, CSIRT Gobierno y Cai virtual Policía Nacional se apoya en la realización de pruebas de vulnerabilidad programadas mínimo una vez al año.

También, la capacitación de los gestores de incidentes cibernéticos del primer respondiente en caso de requerirse en el desarrollo de las tareas y labores de la CIAC.

Con respecto al análisis de log de las rutas críticas de la CIAC se tiene una VPN directamente con el CSIRT Gobierno para este tipo de análisis y revisiones para alertas tempranas.

Bajo herramientas propias de TI se analizan los logs de dispositivos perimetrales de CIAC.

6.3 Aseguramiento de Plataformas

El jefe de infraestructura de GTIC´s junto con los Partner en su momento, de acuerdo al listado firmado y contrato vigente de aliados de soporte de tecnología, inicia un programa anual de aseguramiento de servidores y dispositivos activos de red que requieran las actualizaciones debidas para detectar y proteger las posibles vulnerabilidades que se puedan determinar tempranamente en servidores y plataformas existentes en la CIAC.

7. SENSIBILIZACIÓN EN SEGURIDAD

La principal línea de defensa en materia de seguridad 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 usuario, capacitándole en la necesidad de identificar oportunamente los riesgos de ciberseguridad y todo lo que contempla la seguridad informática, aplicar las políticas de seguridad de la información 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.

7.1 Primeros respondientes incidentes Cibernéticos

Los funcionarios de la corporación del Grupo de GTIC´s, han asistido a los dos encuentros realizados por MINTIC – DIJIN sobre los primeros respondientes ante incidentes cibernéticos –CSIRT Gobierno, con el fin de mejorar las competencias ante cualquier aviso de este tipo de eventos en la CIAC, brindando el apoyo necesario y ser el soporte ante estas instituciones.

7.2 Sensibilización funcionarios

Mediante programación de campañas y/o charlas de sensibilización relacionada con los siguientes temas:

a. Políticas de seguridad de la información
b. Ciberseguridad
c. Servicios de TI
d. Plan estratégico de TI
e. Vulnerabilidades
f. Backup´s
g. Clasificación de la Información y manejo
h. Buenas prácticas de uso de PC´s
i. Pruebas de ingeniería social con Office 365
j. Pruebas de phishing con Office 365

Buscando mejorar el nivel conciencia de cada empleado ya sea de planta y/o contratista se realizan constantemente y cada vez que se requiera el uso de un equipo tecnológico en la corporación la charla obligatoria de Ciberseguridad para personal que ingresa nuevo a la Corporación.

Así mismo, se vienen adelantando charlas para los funcionarios en diferentes escenarios como en reuniones generales, ingreso de funcionarios nuevos, protectores de pantalla, mensajes a través del correo institucional o campañas personalizadas.

8. PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS

La Corporación en su sistema de gestión de calidad mantiene el plan de recuperación de desastre que mínimo una vez al año se actualiza y/o cada vez que se identifica una amenaza potencial o que ponga en riesgo la continuidad del negocio. Sin embargo, GTIC´s mantiene una evidencia de las pruebas de este plan de contingencia que de acuerdo a las necesidades se prueba y/o se activa realizando las siguientes acciones:

8.1 Actualización documentación

Utilizando los mecanismos de estandarización de la Corporación, mantiene la documentación que involucra cada uno de los ítems que compone el PRDT cuando se evidencie cambios en las capacidades tecnológicas, eventos que no estén mencionados en el documento o cambie el mecanismo de puntos que deban estar dentro de este plan ante incidentes tecnológicos que impidan la continuidad de los servicios de las plataformas críticas para la operatividad de los procesos de la Corporación.

8.2 Evidencia Plan de Contingencia Informática

El Grupo de GTIC´S, bajo el documento "Programa de seguridad de la Información" que se encuentra en la plataforma de control de documentos de la CIAC, planea la ejecución de Simulacros para el plan de recuperación de desastres tecnológicos (Seguridad de la Información) evidenciando la acción mediante el formato para este fin.

También puede realizar eventualmente, cuando sea necesario otra prueba, si así, se determina al interior del grupo de GTIC´S (prueba de escritorio), o requiera un cambio en la plataforma y se analice con los aliados y personal de la infraestructura, Coordinador, CIO y /o quienes hagan parte de las demostraciones (en sitio), pero en todo caso se debe dejar la evidencia mostrando los planes de acción y lecciones aprendidas del trabajo efectuado.

9. INVENTARIO ACTIVOS DE INFORMACION

La Corporación de la Industria Aeronáutica Colombiana, realizó el levantamiento de los activos de información por procesos con base en la ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, y se encuentran en cada dependencia claramente establecidos al igual que la consolidación del registro de activos de información publicada en la página WEB.

Está labor es liderada por el proceso de gestión documental que se asocia con las tablas de retención documental bajo las normas establecidas para el tratamiento de la información.

10. PLAN DE COMUNICACIONES

El grupo de Gestión de Tecnologías de la Información y las Comunicaciones, establece un plan de comunicaciones constantemente de sensibilización de los temas de TI, mediante las herramientas tecnológicas como los fondos de pantalla, las charlas informativas, los chats aprobados como Microsoft Teams y también los correos para emitir los comunicados necesarios enviados y que también se pueden programar masivamente a través del SIGTI.

11. ACTIVIDADES VIGENCIA 2022

Ver **PETI 2022**

12. PARTES INTERESADAS

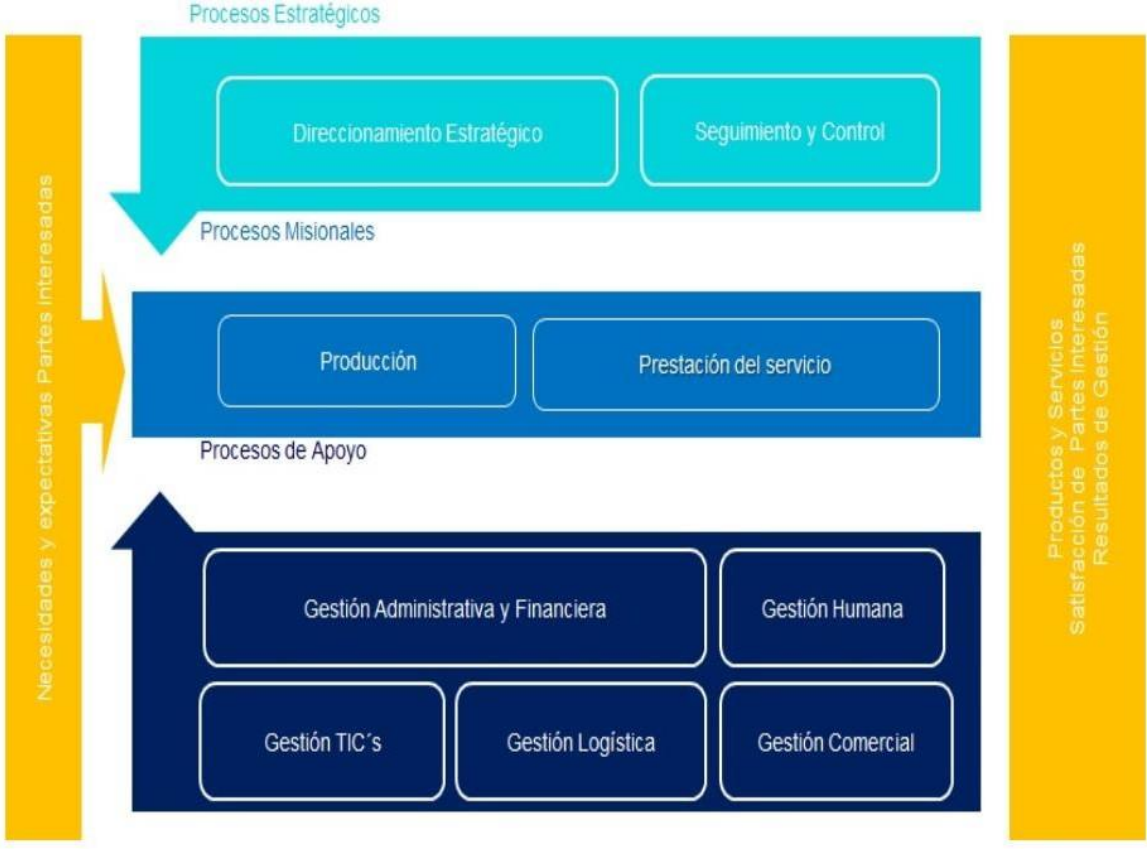
Para El Grupo de GTIC´S dentro de la matriz de partes Interesadas para la Corporación se tiene la siguiente descripción:

MATRIZ DE PARTES INTERESADAS EXTERNAS

Código: MTZ-1-03-001
Fecha de Edición: 26 de septiembre de 2019
Versión: 5

Proceso	Grupo	Partes Interesadas Externas	Necesidades	Expectativas	Actividades
Gestión TIC's	GTICS	Ministerio de Tecnologías de Información y Comunicaciones - MINTIC	•Cumplimiento de Leyes, •Cumplimiento en la directiva y lineamientos del Gobierno Digital.	•Acceso a datos abiertos. •Cumplimiento de los lineamientos emitidos.	•Publicación y actualización de Datos (datos.gov.co) •Documentación solicitada alineada a MINTIC (PETI, Políticas de seguridad, AE, IPV6)
	GTICS	Ministerio de Defensa TICS	Cumplimiento de las Políticas de TI.	•Participación en las reuniones convocadas para el cumplimiento de las políticas TI.	Actualización y cumplimiento del Plan Estratégico de Tecnologías de la Información.
	GTICS	Ministerio de Defensa GSED - CITI	1.Cumplimiento de la Directiva Ministerial permanente N° 013 del 19 de abril de 2013. 2.Acatamiento de las Resoluciones emitidas.	Cumplimiento de plazos y formatos de proyectos de TI.	1.Enviar a tiempo los formatos Citi cuando sean requeridos. 1.Asistir a las sustentación en reuniones para los Proyectos TIC´S vigencias futuras.

Las partes interesadas internas para El Grupo de GTIC´S se encuentra en el siguiente marco del mapa de proceso de la corporación por lo tanto son todos los procesos de la CIAC., así:



13. MATRIZ DE RIESGOS

El grupo de GTIC´s, mantiene el estándar del sistema de Gestión de Riesgos adoptado por la Corporación que contempla los riesgos asociados a las tecnologías de la información y están inmersos en el documento del Manual del Sistema Integral de Gestión del Riesgo y se describen los riesgos uno a uno junto con los

controles prioridades y mapas de calor en la matriz de riesgos para TI en el programa de control de documentos de calidad para la CIAC. (consultar la matriz).