1. OBJETIVO

Identificar las principales amenazas de seguridad y privacidad de la información de acuerdo a los lineamientos y procedimientos impartidos por la Corporación en el Manual del Sistema Integral de Gestión de Riesgos.

2. JUSTIFICACIÓN

Es necesario analizar y controlar cada uno de los riesgos identificados conservando la metodología establecida para garantizar, en lo posible, la seguridad y privacidad de la información, activo valioso para la Corporación.

3. ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información está diseñado para el proceso Gestión Tics.

4. RESPONSABLE

Coordinador de la Oficina de Tecnologias de la Información.
Grupo Gestión TICs.

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 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.

Amenaza: Son aquellos factores externos a la Corporación que advierten proximidad o propensión a un evento de pérdida (materialización de un riesgo) sobre los cuales esta no tiene control.

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

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: 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.

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.

Evento: Incidente o situación que ocurre en un lugar particular en un intervalo de tiempo determinado.

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.

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.

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.

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.

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. METODOLOGIA

La metodología establecida para la elaboración de los Mapas de Riesgos es la establecida en el Manual del Sistema Integral de Gestión de Riesgos CIAC.

7. ROLES Y RESPONSABILIDADES

Coordinador GTIC´s

- Identificar, analizar, evaluar y controlar los riesgos que afecten la seguridad y privacidad de la información 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 del mismo.

Colaboradores GTICS

- Acorde al organigrama del Grupo de Gestión Tics, cada uno de los funcionarios 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 SO de cada uno de los servidores acorde a las publicaciones del fabricante.

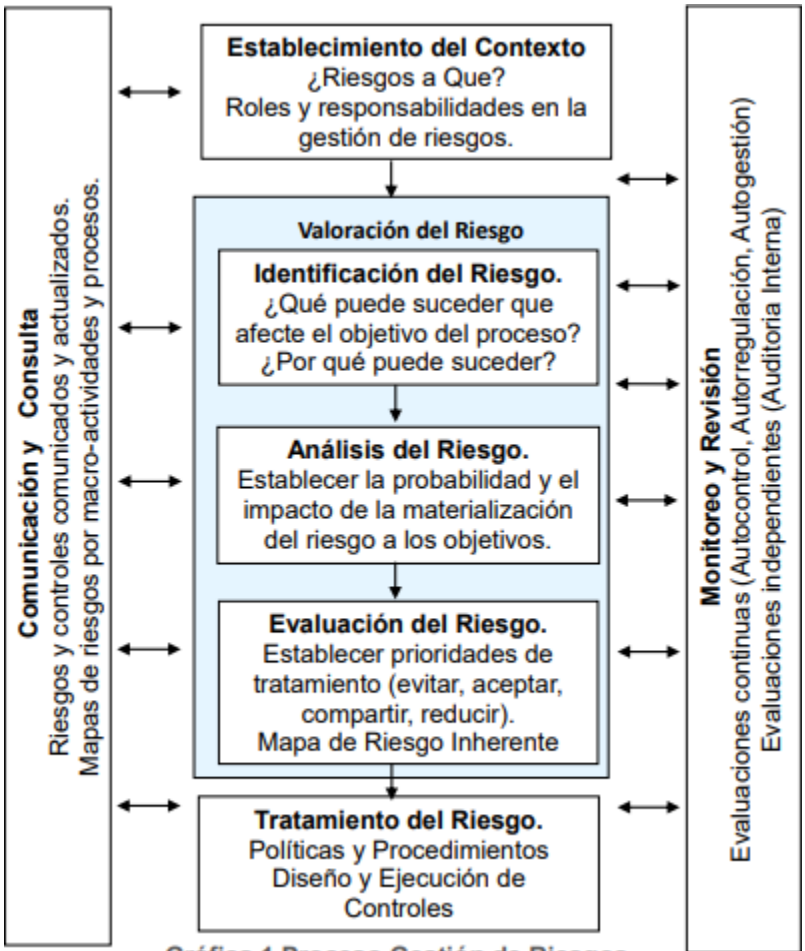
- Conocer y aplicar las políticas de seguridad de la información.

- Mantener informado al Coordinado de Gtics, 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 a 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.

8. PROCESO DE GESTION DEL RIESGO



Gráfica 1 Proceso Gestión de Riesgos

Fuente: Manual del Sistema Integral de Gestión de Riesgos CIAC.

9. ESQUEMA DEL MAPA DE RIESGOS Y SEVERIDAD DEL RIESGO

A continuación, se presenta el mapa de riesgos adoptado por la Corporación y el esquema del mapa de riesgos con los niveles de probabilidad de ocurrencia y magnitud del impacto.

- La dimensión del mapa corresponde a niveles de 5 filas por 5 columnas que brindan mayor flexibilidad en la determinación de los riesgos intermedios.

- El mapa de riesgos corresponde a una estructura no lineal, para establecer un mayor peso a aquellos eventos, causas o fallas en los cuales, aunque la probabilidad es baja, su impacto al interior para la CIAC es crítico.

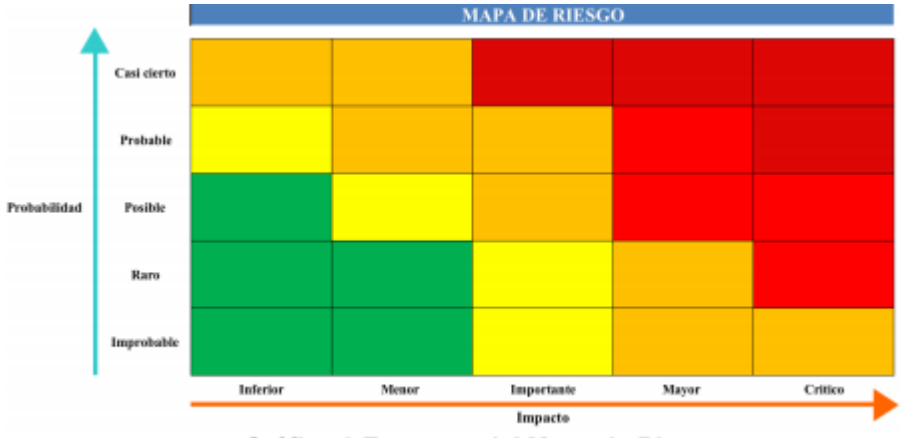


Gráfico 2 Esquema del Mapa de Riesgos

A su vez, la combinación de la probabilidad de ocurrencia y magnitud del impacto del riesgo, permiten determinar el nivel de riesgo del Proceso conocido como perfil de riesgo:

Gráfico 3 Severidad del Riesgo

10. CRITERIOS PARA LA CALIFICACIÓN DE PROBABILIDAD E IMPACTO

Para la calificación de riesgos, la Corporación ha definido una serie de criterios de calificación de probabilidad e impacto, con el objetivo de homogenizar esta actividad a lo largo de la Corporación y sus Procesos. Estos criterios son revisados, ajustados y aprobados anualmente teniendo en cuenta los cambios en la Organización, los resultados financieros de la Corporación y las nuevas estrategias y/o proyectos en los que se involucre la CIAC.

10.1 Posibilidad de Ocurrencia – Probabilidad

Nivel	Periodicidad	Frecuencia
Casi Cierto	Recurrente - Se espera que el evento pueda ocurrir con cierta periodicidad - 1 vez cada mes	Se espera la ocurrencia del evento en más del 20% de los casos
Probable	Frecuente. Se espera que el evento pueda presentarse 1 vez cada trimestre	El evento puede ocurrir entre el 15 y el 20% de los casos
Posible	Posible. Se espera que el evento pueda presentarse 1 vez cada semestre	El evento puede ocurrir entre el 10 y 14.99% de los casos
Raro	Ocasional. Se espera que el evento pueda presentarse 1 vez en el año	El evento puede ocurrir entre el 3 y el 9.99% de los casos
Improbable	Improbable - El evento se ha presentado 1 vez en los últimos años	El evento puede ocurrir en menos del 3% de los casos

Impacto

DESCRIPCIÓN	
Crítico	Seguridad de la Información: Pérdida de información crítica propia o de terceros que no se pueda recuperar o utilización indebida de información sensible de los clientes
Mayor	Pérdida de información crítica de la CIAC o de terceros que no se pueda recuperar fácilmente, ocasionando retrasos en las labores de las áreas, respuesta a los entes reguladores y a los clientes.
Importante	Falta de disponibilidad de la información, ocasionando retrasos en las labores de las áreas y/o en la respuesta a los clientes Continuidad: Interrupción de las operaciones entre 24 y 47 horas continúas.
	No afecta la oportunidad de la información de manera significativa, no altera el

Menor	funcionamiento de las áreas receptoras y procesadoras de información. Continuidad: Interrupción de las operaciones menor a 24 horas continúas.
Inferior	No afecta la oportunidad de información Continuidad: No hay interrupciones de las operaciones

Apetito al Riesgo

La entidad tiene como objetivo mantener como máximo un nivel de exposición moderado en los riesgos identificados, ello sin limitación de desarrollar por parte de los diferentes Procesos y Dependencias planes de acción para implementación de los controles de los riesgos moderados y bajos. El siguiente cuadro detalla el riesgo objetivo de acuerdo a los niveles aceptables.

Nivel de Exposición Actual	Nivel de Riesgo Objetivo
Extremo	Moderado
Alto	Moderado
Moderado	Bajo
Bajo	Bajo

Gráfico 4 Apetito al Riesgo

Tolerancia al Riesgo

La tolerancia al riesgo son los niveles aceptables de desviación relativa a la consecución de objetivos operacionales para cada proceso. Todos los objetivos operacionales deben tener una tolerancia máxima permitida y deberá ser expresada en alguna unidad de medición en función de los indicadores establecidos para cada proceso.

Como resultado de la etapa de Establecimiento del Contexto, la Corporación cuenta con los siguientes elementos:

- Lista de los objetivos operacionales de todos los procesos.
- Criterios de Calificación de Riesgos (probabilidad e impacto).
- Apetito al riesgo con el nivel de riesgos deseado por la Corporación.
- Tolerancia al riesgo de los objetivos operacionales identificados.

11. VALORACIÓN DEL RIESGO

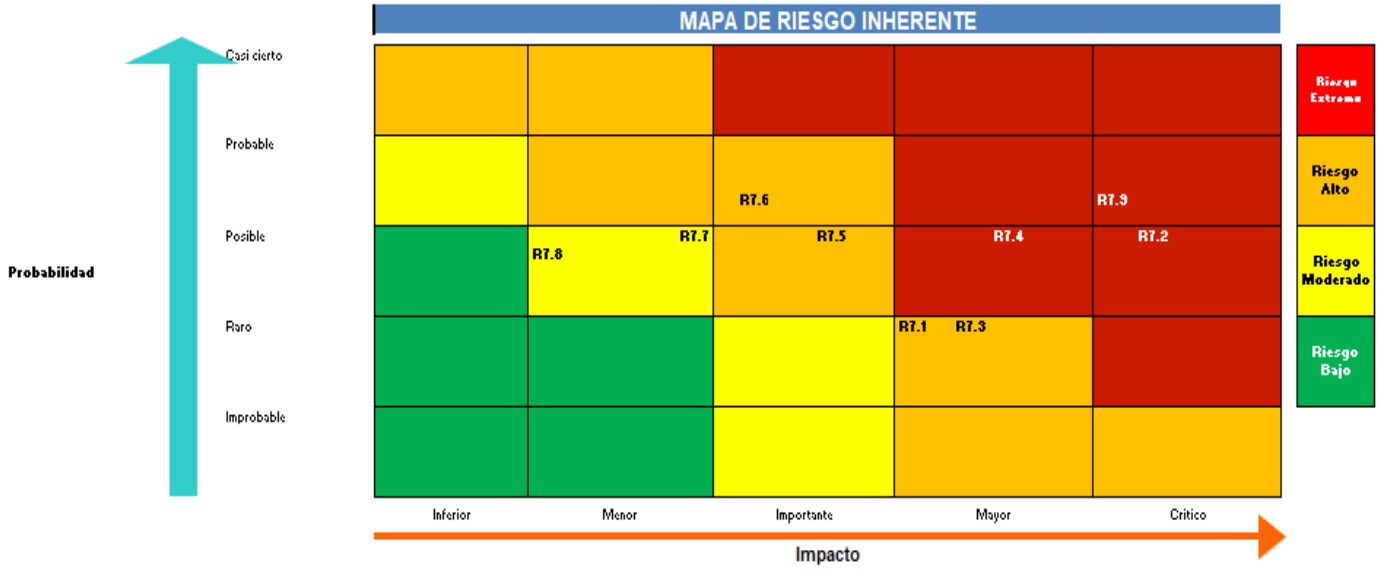
La valoración del riesgo contempla las actividades de identificación, análisis y evaluación de riesgos y se puede consultar en el Manual de tratamiento de riesgos general para la CIAC.

Tipología del Riesgo

Tipo de Riesgo	Definición
Riesgo de Seguridad de la Información (RSI	Es la posibilidad de no cumplir con las características de confidencialidad, integridad y disponibilidad de la información, así como otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad que pueden estar involucradas en los activos de información de la entidad.

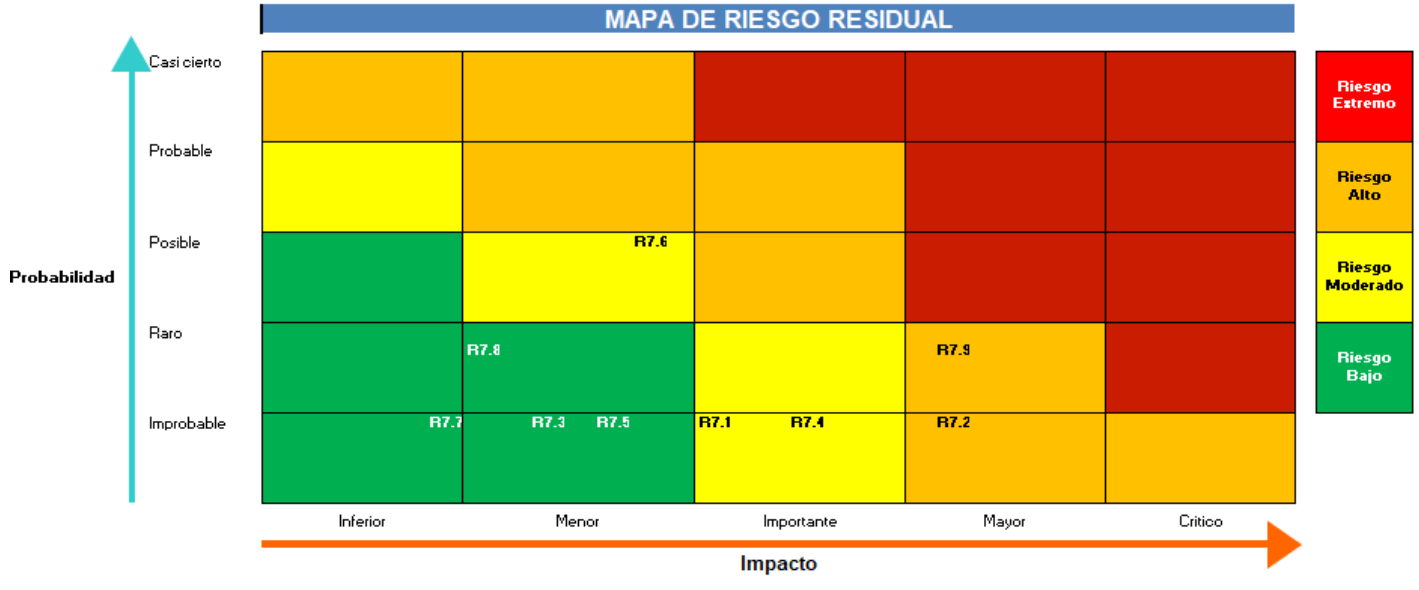
Para la matriz de riesgos y los controles referentes a la seguridad y privacidad de la información, la matriz de riesgos arroja los siguientes mapas de calor:

Sin controles:



Los datos pueden ser consultados a través del programa controlado dentro de la Corporación que por ser formulado no se puede anexar al plan, pero si hace parte del presente.

Aplicando Controles:



Riesgos y Controles:

A continuación, se describen los riesgos referentes a la seguridad y privacidad de la información a modo de ejemplo, ya que se encuentran plenamente identificados en la Matriz de riesgos para el proceso Gestión TIC's.

Proceso: **Gestión TICs**

Mapa Consolidado e Individual por Tipologia de Riesgo

Proceso (Gerencial / Misional / Apoyo)	Proceso	Riesgo #	Riesgos del Proceso	TIPOLOGIA DE RIESGO							Causas y/o Fallas	Factor de riesgo
				RO	RC	RLAFT	RF	RSI	RSST	RA		
Apoyo	Gestión TICS	R7.1	Implementación de políticas de Tecnologías de Información y Comunicaciones no alineadas con la normatividad vigente (Normatividad emitida por MINTIC).	Si	No	No	No	Si	No	No	Desconocimiento de la normatividad vigente (guías y lineamientos de MINTIC)	Recurso Humano
Apoyo	Gestión TICS	R7.1	Implementación de políticas de Tecnologías de Información y Comunicaciones no alineadas con la normatividad vigente (Normatividad emitida por MINTIC).	Si	No	No	No	Si	No	No	Desconocimiento de la normatividad vigente (guías y lineamientos de MINTIC)	Recurso Humano
Apoyo	Gestión TICS	R7.1	Implementación de políticas de Tecnologías de Información y Comunicaciones no alineadas con la normatividad vigente (Normatividad emitida por MINTIC).	Si	No	No	No	Si	No	No	Inadecuado analisis y adaptación de los requerimientos a cumplir.	Recurso Humano
Apoyo	Gestión TICS	R7.1	Implementación de políticas de Tecnologías de Información y Comunicaciones no alineadas con la normatividad vigente (Normatividad emitida por MINTIC).	Si	No	No	No	Si	No	No	Insuficiencia de recursos para el cumplimiento de los requerimientos normativos y políticas de gobierno de MINTC (físicos, humanos, etc)	Recurso Humano
Apoyo	Gestión TICS	R7.1	Implementación de políticas de Tecnologías de Información y Comunicaciones no alineadas con la normatividad vigente (Normatividad emitida por MINTIC).	Si	No	No	No	Si	No	No	Insuficiencia de recursos para el cumplimiento de los requerimientos normativos y políticas de gobierno de MINTC (físicos, humanos, etc)	Recurso Humano
Apoyo	Gestión TICS	R7.2	Pérdida de integridad de la plataforma tecnológica de la CIAC	Si	No	No	Si	Si	No	No	Implementación de cambios no autorizados por la CIAC a los aplicativos de la plataforma tecnológica.	Recurso Humano

Nota: La anterior información se encuentra en la plataforma de control documental Isolución, y es propiedad de la Corporación de la Industria Aeronáutica Colombiana S.A., haciendo y hace parte de la Documentación confidencial.

12. CONTROL DE CAMBIOS

REVISIÓN	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE	FECHA
1	Emisión del documento	Coordinador Grupo de Gestión TICS	27/Jul/2018
2	Actualización numeración	Coordinador Grupo de Gestión TICS	26/Abr/2019
3	Actualización contenido general	Coordinador Grupo de Gestión TICS	16/Ene/2020

ELABORÓ	REVISÓ	APROBÓ
Nombre: Alexander Martinez Ortiz **Cargo:** Coordinador Sistemas **Fecha:** 22/Ene/2020	**Nombre:** CR (RA) Alvaro Molano **Cargo:** Jefe Oficina de Planeación, Innovación y Desarrollo **Fecha:** 28/Ene/2020	**Nombre:** BG Iván Delascar Hidalgo Giraldo **Cargo:** Gerente General **Fecha:** 28/Ene/2020