Guía

COM-G-9

Guía de orientación para la elaboración de las tablas de control de acceso (TCA)

Instituto Caro y Cuervo

Proceso de Información y comunicación

25/08/2025

TABLA DE INFORMACIÓN DEL DOCUMENTO

Versión	Fecha de aprobación	Elaborado	Revisado	Aprobado	Descripción del cambio
1.0	09/10/2024	Alix Lorena Moreno Córdoba Contratista - Oficial de seguridad de la información	Leidy Tatiana Vela Garces Contratista- Grupo de Gestión Documental Cristian Armando Velandia Mora – Coordinador del Grupo de Planeación y Relacionamiento con el Ciudadano William Javier Rodríguez Salcedo – Rol abogado jurídico	Jorge David Sabogal Jiménez- Coordinador Grupo de Gestión Documental	Versión inicial del documento
2.0	25/08/2025	Leidy Tatiana Vela Garces- Contratista Grupo de Gestión Documental	Alix Lorena Moreno Córdoba Contratista - Oficial de seguridad de la información.	Jorge David Sabogal Jiménez- Coordinador Grupo de Gestión Documental	Ajuste en el campo de Nivel de Riesgo, este ajuste se realiza para alinear la clasificación del Nivel de riesgo con el Índice de Información Clasificada y Reservada, utilizando el promedio de los valores de disponibilidad, integridad y confidencialidad (CID).

ÍNDICE DE CONTENIDO

INTRODUCCIÓN 5
1 OBJETIVO 5
1.1 Objetivos específicos 5
2 ALCANCE 6
3 TÉRMINOS Y DEFINICIONES 7
4 REQUERIMIENTOS PREVIOS DE CONTROL DE ACCESO Y SEGURIDAD PARA LOS DOCUMENTOS 8
5 CONTROL DE ACCESO Y SEGURIDAD PARA LOS ARCHIVOS Y DOCUMENTOS 12
5.1 Articulación del Plan Institucional de Archivos - PINAR - con los sistemas de gestión 12
5.2 Análisis normativo en el control de acceso y seguridad 14
5.3 Roles y responsabilidades para el control de acceso y seguridad 15
5.4 Documentación y comunicación 16
5.5 Análisis de actividades del ICC y su articulación con la caracterización de procesos 16
5.6 Análisis de los activos de información y su articulación con las tablas de retención documental (TRD) 17
5.7 Análisis de riesgos 17
5.8 Análisis de usuarios 18
5.9 Seguimiento y mejora 18
6 TABLAS DE CONTROL DE ACCESO (TCA) 18
6.1 Diferencia TCA y el índice de información clasificada y/o reservada 18
6.2 Calificación de la información 19
6.3 Permisos sobre los archivos y documentos 19
6.4 Formato de tabla control de acceso (TCA) 19
6.4.1 Revisión, aprobación y actualización 22
6.4.2 Divulgación de las tablas de control de acceso 22
7 CONCLUSIONES Y RECOMENDACIONES 22
8 FORMATOS ASOCIADOS 23

ÍNDICE DE TABLAS

Tabla 1 Requisitos previos para la implementación de las TCA 8
Tabla 2 Requerimiento instrumentos archivísticos....8
Tabla 3 Requerimiento directrices de sistemas y tecnología 9
Tabla 4 Requerimiento de recursos 10
Tabla 5 Requerimiento normatividad y asuntos jurídicos....11
Tabla 6 Articulación PINAR con el SIG....13
Tabla 7 Roles para el control de acceso y seguridad 15
Tabla 8 Información para la caracterización de procesos....16
Tabla 9 Campos para diligenciar en el formato....19
Tabla 10 Ejemplo de diligenciamiento tabla de control de acceso....21

ÍNDICE DE FIGURAS

Figura 1 Ecosistema control de acceso 12

INTRODUCCIÓN

En cumplimiento con el Decreto 1078 de 2015, que define el componente de seguridad de la información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo debe estar alineado con la gestión documental de la entidad, conforme a los parámetros emitidos por el Archivo General de la Nación (AGN), definidos en él Modelo de Gestión Documental y Administración de Archivos, y del Decreto 1080 de 2015, artículo 2.8.2.5.8 sobre Instrumentos archivísticos para la gestión documental. Dentro de estos instrumentos se encuentra el documento presente, específicamente denominado Tablas de Control de Acceso (TCA).

Las Tablas de Control de Acceso (TCA) son instrumentos fundamentales para implementar políticas, directrices y medidas de seguridad destinadas a proteger la información contra el acceso, recolección, divulgación, eliminación, alteración y/o destrucción no autorizada. Este documento establece los requisitos previos para las diferentes categorías de clasificación de la información, define y asigna responsabilidades de seguridad, uso y acceso a la misma. La construcción de este documento se basa en el Anexo A de la norma ISO 27001:2013, específicamente en el objetivo de control A.9 Control de acceso, y en la guía de derechos y restricciones de acceso y seguridad aplicables a los documentos electrónicos.

1 OBJETIVO

Proporcionar las directrices desde el Sistema de Gestión de Seguridad de la Información (SGSI) para el establecimiento de las categorías adecuadas de derechos y restricciones de acceso y seguridad a través de la orientación en la implementación del control de acceso para los documentos del Instituto Caro y Cuervo (ICC) con el fin de protegerlos y garantizar el acceso a la información por los ciudadanos y grupos de interés.

1.1 Objetivos específicos

a. Identificar los requerimientos previos a la elaboración e implementación de las tablas de control de acceso (TCA).
b. Identificar los elementos normativos y jurídicos que influyen en la valoración de seguridad y acceso a los archivos y documentos.
c. Gestionar las principales amenazas y vulnerabilidades de seguridad de la información que enfrenta la Entidad en relación con la protección y acceso a la información.
d. Definir los niveles de confidencialidad aplicables a los archivos y documentos, estableciendo restricciones o privilegios.

2 ALCANCE

Inicia con la revisión de los requerimientos previos que se deben tener en cuenta antes de elaborar las TCA, continúa con la orientación y articulación de los elementos que proporciona el Sistema de Gestión de Seguridad de la Información (SGSI) tales como la identificación, calificación y valoración de activos, la gestión de riesgos, las políticas de seguridad y privacidad de la información y finaliza con las sugerencias y buenas prácticas realizadas desde el SGSI para el control de acceso en documentos y archivos tanto en soporte análogo como digital.

Las recomendaciones presentadas en este documento no eximen ni limitan el cumplimiento de las disposiciones jurídicas y normativas. Por el contrario, deben alinearse garantizando los controles necesarios para la protección de archivos y documentos, con el objetivo de asegurar la eficiencia, la eficacia y la transparencia en la gestión.

Este documento orientará al Grupo de Gestión Documental en el manejo de archivos y documentos específicamente para el control de acceso, seguridad y consulta de los documentos ofrecidos a través de sistemas de información, servicios tecnológicos y los archivos análogos.

3 TÉRMINOS Y DEFINICIONES

- **Caracterización de procesos**: Actividad usada para realizar un análisis profundo de los procesos teniendo en cuenta los elementos que originan que estos procesos tengan un principio y un final.
- **Control de acceso a documentos y archivos:** Conjunto de políticas de seguridad de la información, procedimientos, controles y medidas de seguimiento que se implementan para permitir el acceso solo a usuarios autorizados y para proteger la información de alteración y/o destrucción no autorizada.
- **Grupos de interés:** personas naturales (ciudadanos) o jurídicas (organizaciones públicas o privadas) a quienes van dirigidos los bienes y servicios de una entidad. (Función Pública, 2018).
- **Índice de información clasificada y/o reservada:** es un documento o herramienta que se utiliza para catalogar y gestionar la información que ha sido clasificada por su sensibilidad.
- **Metadatos:** Información estructurada o semi-estructurada que posibilita la creación, registro, clasificación, acceso, conservación y disposición de los documentos a lo largo del tiempo.
- **Programa de Gestión Documental - PGD:** Instrumento archivístico que formula y documenta a corto, mediano y largo plazo, el desarrollo sistemático de los procesos archivísticos, encaminados a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por una entidad, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.
- **Plan Institucional de Archivos- PINAR:** Instrumento para la planeación de la función archivística, el cual se articula con los demás planes y proyectos estratégicos previstos por el ICC.
- **Registro de activos de información:** es un documento o herramienta que permite identificar, clasificar y gestionar todos los activos de información dentro de una organización.
- **Tablas de Control de Acceso - TCA:** Instrumento para implementar políticas, directrices y medidas de seguridad que permitan proteger la información, así como garantizar el acceso a la información por los ciudadanos y los grupos de interés.

4 REQUERIMIENTOS PREVIOS DE CONTROL DE ACCESO Y SEGURIDAD PARA LOS DOCUMENTOS

Previa implementación de las tablas de control de acceso (TCA) es preciso realizar una identificación de las actividades ya realizadas en el ICC con el objetivo de articular y alinear estas directrices con el sistema de gestión de seguridad de la información y la gestión documental.

Tabla 1 Requisitos previos para la implementación de las TCA

Requerimiento	Sistema Integrado de Gestión (SIG)
Responsable	Grupo de Planeación y Relacionamiento con el Ciudadano
Descripción	**Evidencia o comentario**
Objetivos misionales de la organización	Enlace el Plan Estratégico Institucional (PLEI)
Caracterización de los procesos y procedimientos de la organización	Enlace al SIG - Sistema Integrado de Gestión
Plan de Acción Institucional	Enlace al portal de Transparencia Numeral 4.3 Plan de Acción
Procedimiento de Auditoría y Seguimiento	Enlace al procedimiento EVA-P-1 Auditoría interna de gestión
Metodología para el análisis y gestión de riesgos, establecida por la organización y los resultados del análisis de riesgos institucionales junto con las acciones de mitigación y gestión de los riesgos	Política de riesgos en el DIR-M-1 Manual administración del riesgo en el Enlace al SIG - Sistema Integrado de Gestión

Tabla 2 Requerimiento instrumentos archivísticos

Requerimiento	Instrumentos archivísticos
Responsable	Grupo de Gestión Documental
Descripción	**Evidencia o comentario**
El cuadro de clasificación documental articulado con: a) Soporte y formato en que se encuentra la información, archivos y documentos de las series y subseries documentales. b) Metadatos y descriptores de las series y subseries documentales.	a) **Registro de activos de información y el Índice de información clasificada y reservada**: Información encontrada en la página del ICC, transparencia y acceso a la información pública, numeral *7.1. Instrumentos de gestión de la información,* numerales 7.1.1 y 7.1.2; respectivamente b) El entregable sugerido es el documento de requerimientos funcionales del SGDEA acorde con este Enlace al modelo de requisitos del AGN.
Tabla de Retención Documental (TRD).	Enlace a Tablas de Retención Documental (TRD)

Requerimiento	Instrumentos archivísticos
Responsable	Grupo de Gestión Documental
Descripción	**Evidencia o comentario**
Programa de Gestión Documental (PGD).	Enlace al Programa de Gestión Documental (PGD) Instrumento archivístico de modo operativo que formula el desarrollo de los distintos procesos llevados a cabo bajo el concepto de archivo total en el ICC.
Plan Institucional de Archivos de la Entidad (PINAR).	Enlace al Plan Institucional de Archivos del ICC (PINAR) Permite al ICC ejecutar, diseñar, implementar, controlar y mejorar los procesos de Gestión Documental para la administración de la información en la entidad de forma eficiente
Inventario Documental.	El Grupo de Gestión Documental ha avanzado en la elaboración de un inventario documental. Sin embargo, debido a la falta de información precisa sobre el volumen total de documentos, resulta complicado proporcionar porcentajes reales.
Mapas de procesos, procedimientos documentales y la descripción de las funciones de las unidades administrativas de la entidad	De acuerdo con el PGD, el Grupo de Gestión Documental elaborará procedimientos que permitan optimizar el manejo de información, mejorando la operativa y asegurando la integridad de los datos. Para ello, se dispone de los procedimientos y documentación del proceso de *Información y Comunicación* que puede consultarse en Enlace al SIG. Además, la descripción de funciones se encuentra en el Acuerdo 002 de 2010 del ICC y en la Resolución 290 de 2022 del ICC.

Tabla 3 Requerimiento directrices de sistemas y tecnología

Requerimiento	Directrices de sistemas y tecnología
Responsable	Grupo de Tecnologías de la Información (TI)
Descripción	**Evidencia o comentario**
Políticas de tecnologías de la Información para control de acceso a los sistemas de información y redes de la Entidad.	En el ICC se tienen los instrumentos de DIR-M-2 Manual de Políticas de Seguridad y Privacidad de la Información.

Requerimiento	Directrices de sistemas y tecnología
Responsable	Grupo de Tecnologías de la Información (TI)
Descripción	**Evidencia o comentario**
• Actividades para la asignación de roles y perfiles • Actividades para otorgar acceso al esquema de red corporativo • Actividades para otorgar acceso a carpetas compartidas	También se da lineamientos a través de la COM-G-6 Guía para la creación de cuentas de red y correo electrónico. El entregable sugerido es el procedimiento para la gestión de los accesos a los servicios tecnológicos que ofrece el Instituto, que se encuentra en construcción, este debe articularse con la gestión realizada en OneDrive por los usuarios.
Los requisitos del negocio para el control de acceso definidos por el Sistema de Gestión de Seguridad de la Información.	Enlace al plan de seguridad y privacidad de la información
Información y políticas del directorio activo.	Son las definidas en el procedimiento para la gestión de accesos
Inventario esquemático de los sistemas de información de la institución, con la descripción funcional y de almacenamiento, identificando la relación con las series y subseries documentales de la TRD. (Este inventario debería relacionarse con las series documentales en el Cuadro de Clasificación Documental de la Entidad)	El entregable sugerido es el catálogo de sistemas de información conforme a con lo indicado en la Enlace a la guía para construir un catálogo de sistemas el cual debe ir articulado con las tablas de retención documental.

Tabla 4 Requerimiento de recursos

Requerimiento	Recursos
Responsable	Grupo de Gestión Documental
Descripción	**Evidencia o comentario**
Conformar un equipo de trabajo interdisciplinario con personal en gestión documental, sistema integrado de gestión, tecnología, jurídica y personal de acuerdo con los procesos de negocio que se estén analizando.	Resolución 132 del 2021: Equipo técnico de la dimensión Información y Comunicación, en su política de gestión documental, el coordinador de gestión documental es quien debe convocar las reuniones de este equipo. Enlace al SIG - Resolución 132 de 2021
Información, archivos y documentos de los procesos de la organización, de acuerdo con las etapas de ciclo vital de los documentos, Archivos de Gestión, Central, Intermedios e Histórico.	Enlace al SIG - Proceso de Información y Comunicación

Tabla 5 Requerimiento normatividad y asuntos jurídicos

Requerimiento	Normatividad y asuntos jurídicos
Responsable	Dirección General – Rol jurídico externo
Descripción	**Evidencia o comentario**
Normograma institucional aplicado a la regulación del objeto social y los procesos de la organización. El objetivo es tener un marco legal para conocer los derechos y responsabilidades atinentes al acceso y seguridad de la información.	El entregable sugerido es la matriz legal del ICC en donde se incluyan todas las normas relacionadas a seguridad digital y de la información. Este documento se puede consultar en los documentos de interés del SIG.
Normas internas que reglamentan los procesos.	El entregable sugerido es la matriz legal de la Entidad en donde se incluyan todas las normas relacionadas a seguridad digital y de la información
Acuerdos de confidencialidad	Funcionarios y contratistas cuentan con cláusulas de confidencialidad firmadas.
Antecedentes de procesos jurídicos por acceso o seguridad de la información.	Hasta la fecha no se han presentado procesos jurídicos relacionados con este tema.

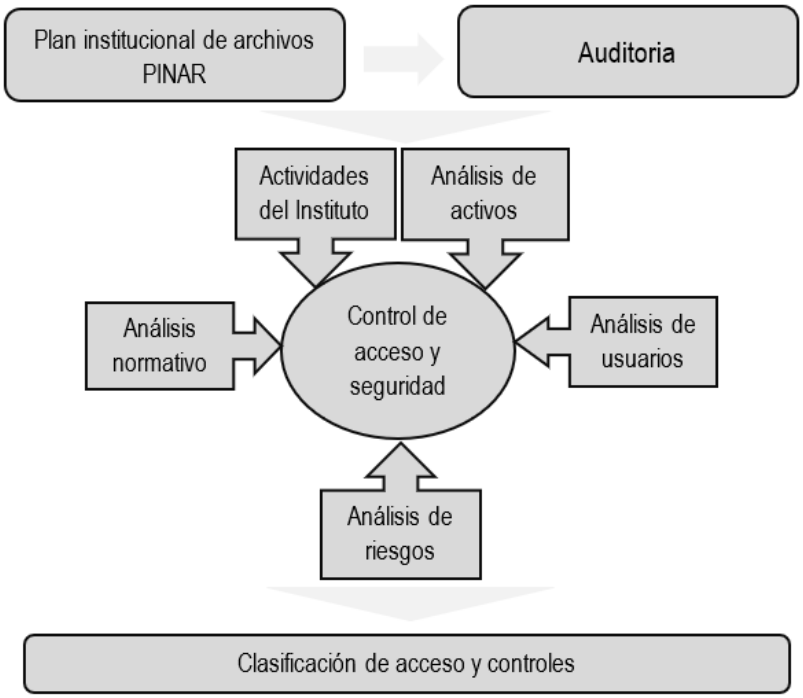
5 CONTROL DE ACCESO Y SEGURIDAD PARA LOS ARCHIVOS Y DOCUMENTOS

A través del control de acceso se determinan los permisos y privilegios que se otorgan sobre los archivos y documentos, así como a los usuarios, es decir que responsabilidades y acciones se puede realizar en relación con un activo (archivos, documentos e información).

Es importante identificar por cada activo de información el nivel de confidencialidad asignado, que se refiere a la protección de la información contenida en los archivos y documentos.

A continuación, se identifican los principales elementos para el control de acceso

Figura 1 Ecosistema control de acceso



Fuente: Infoesfera, Derechos y restricciones de acceso y seguridad aplicables a los documentos electrónicos. Jhon A. Gonzalez. F

5.1 Articulación del Plan Institucional de Archivos - PINAR - con los sistemas de gestión

El PINAR es un instrumento para la planeación de la función archivística, el cual se articula con los demás planes y proyectos estratégicos previstos por el Instituto Caro y Cuervo, el objetivo de articular los sistemas de gestión con las políticas y directrices del control de acceso y seguridad de los archivos y

documentos consiste en optimizar recursos y evitar realizar actividades desarticuladas al interior de la Entidad, por lo anterior se presentan las siguientes herramientas que ya se tienen implementadas por parte de los sistemas de gestión:

Tabla 6 Articulación PINAR con el SIG

Elemento	Descripción	Gestión documental
Declaración de Política[1] de control de acceso	Política actual: El Grupo de las TI debe implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, carpetas compartidas, bases de datos y servicios tecnológicos, en cuanto a la definición de procedimientos para mantener el acceso controlado físico a las instalaciones de la Entidad el Grupo de Recursos Físicos es responsable. Estos procedimientos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.	Apoyar en la elaboración de la guía para el control de acceso y seguridad de archivos y documentos en formato físico, que debe incluirse en la política de control de acceso definida en el manual de políticas de seguridad de la información.
Procesos y procedimientos	Se cuenta con el sistema integrado de gestión con un mapa de procesos actualizado.	Elaborar y normalizar los formatos y registros vinculados a la evidencia de la implementación de los controles de acceso, consulta y préstamos.
Mejora continua	Se cuenta con el procedimiento de reportes de eventos e incidentes de seguridad de la información, la gestión de riesgos y los indicadores del SGSI.	Establecer las acciones correctivas, preventivas y de mejoramiento para garantizar el cumplimento de los requisitos del control de acceso y seguridad.
Seguimiento y control	Se cuenta con los indicadores para la medición del funcionamiento del sistema de gestión de seguridad de la información.	Establecer indicadores articulados con el SGSI que permitan validar la eficacia de los controles de acceso definidos.
Auditoría	Se realizan auditorías por parte de la Unidad de Control Interno, las cuales proporcionan el insumo para la suscripción de un plan de mejora.	Incluir la verificación de los requisitos de control de acceso y seguridad en los planes de auditoría de la Entidad.

[1] Instituto Caro y Cuervo - Manual de políticas de seguridad de la información Enlace al manual de políticas de seguridad y privacidad de la información

5.2 Análisis normativo en el control de acceso y seguridad

Este análisis busca entender el marco jurídico aplicable al ICC y sus procesos para determinar la claridad en los derechos y responsabilidades frente a la producción, consulta, acceso y seguridad de los archivos y documentos que, en cumplimiento de sus funciones, produce, gestiona y almacena. Este análisis servirá en el proceso de calificación y valoración de los activos de información y como fuente de información para el análisis y valoración de los riesgos de seguridad de la información.

Normatividad y lineamientos de acceso a la información:

- **Constitución Política de Colombia, artículo 74:** "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley. El secreto profesional es inviolable."
- **Ley 594 de 2000:** Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones
- **Ley 1266 de 2008**: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **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 dictan otras disposiciones
- **Decreto 1080 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- **Acuerdo 001 de 2024:** "Por el cual se establece el Acuerdo Único de la Función Archivística, se definen los criterios técnicos y jurídicos para su implementación en el Estado Colombiano y se fijan otras disposiciones.
- **DIR-M-2 Manual de políticas de seguridad y privacidad de la información:** Establece los lineamientos para proteger los activos de información y los datos personales teniendo en cuenta los requisitos legales y la norma ISO 27001:2013.
- **DIR-M-16 Manual de política de Gestión documental:** Proporcionar lineamientos que permitan una adecuada gestión documental en el ICC que se enfoque en la eficiencia de las actividades de la función archivística, protección al patrimonio documental y promoción de la transparencia, acceso y seguridad a la información por parte de la ciudadanía.

5.3 Roles y responsabilidades para el control de acceso y seguridad

La siguiente tabla describe los roles y responsabilidades clave en el proceso de control de acceso y seguridad dentro del ICC. Cada rol tiene funciones específicas orientadas a garantizar que las políticas de seguridad de la información sean implementadas de manera efectiva, que el personal esté adecuadamente informado y que los procedimientos de gestión de la información se alineen con las normativas vigentes. Esta estructura permite una coordinación eficaz entre los diferentes actores responsables de la protección de los activos de información, promoviendo una cultura de seguridad y responsabilidad compartida.

Tabla 7 Roles para el control de acceso y seguridad

Rol	Responsabilidad
Oficial de seguridad de la información	✓ Asegurar que las políticas sean comunicadas y entendidas por todo el personal. ✓ Fomentar una cultura de seguridad en la organización mediante campañas de concientización. ✓ Actuar como punto de contacto para consultas en temas de seguridad de la información.
Coordinador del grupo de Gestión Documental	✓ Garantizar que las prácticas de gestión documental se alineen con las normativas y políticas de control de acceso y seguridad de la información. ✓ Colaborar con el Oficial de Seguridad de la Información y los grupos de trabajo para asegurar una integración efectiva de las políticas de control de acceso. ✓ Asegurar que los procedimientos sean accesibles y comprensibles para todo el personal involucrado.
Propietario custodio de la información	✓ Trabajar junto con otros roles, como el Oficial de Seguridad de la Información y el Grupo de Gestión Documental, para asegurar un enfoque integral en la seguridad de la información. ✓ Fomentar una cultura de responsabilidad en el manejo de la información. ✓ Revisar y aprobar solicitudes de acceso, asegurando que estén alineadas con las políticas de seguridad. ✓ Asegurar que las políticas de control de acceso y seguridad sean correctamente implementadas en la gestión de la información bajo su responsabilidad.

5.4 Documentación y comunicación

El Grupo de Gestión Documental es responsable de consolidar la información de los diferentes grupos de trabajo, contando con el apoyo del profesional de seguridad de la información. Una vez que se haya recopilado la información completa, se presentará ante el Comité Institucional de Gestión y Desempeño (CIGD) para su aprobación y posterior publicación en la página web del ICC. Además, el Grupo deberá comunicar esta información a los grupos de trabajo que actúan como custodios de esta.

5.5 Análisis de actividades del ICC y su articulación con la caracterización de procesos

Este análisis se refiere al entendimiento de los procesos del ICC, identificando insumos, procedimientos y salidas. La caracterización de estos procesos, realizada a través del Sistema de Gestión de Calidad, proporciona la información necesaria para entender cómo se desarrollan y gestionan dentro del Sistema Integrado de Gestión (SIG).

Tabla 8 Información para la caracterización de procesos

Caracterización de procesos						
Información del Proceso (objetivo, alcance y responsables)	Información de Identificación (Codificación, versión, fecha)	Proveedores	Entradas	Ciclo PHVA	Salidas	Usuarios
Recursos			Documentos		Indicadores	

La caracterización de procesos permite al ICC obtener una visión integral de cada actividad, facilitando la identificación y gestión eficiente de la información, documentos y archivos involucrados. A través de esta herramienta, es posible:

- Determinar qué información, documentos y archivos se requieren como insumo para el proceso.
- Identificar los documentos que se generan o se integran durante el desarrollo del proceso.
- Establecer los documentos resultantes o insumos para otros procesos.
- Evaluar la relevancia de los documentos tanto para el proceso en cuestión como para la Entidad en su conjunto.
- Identificar los proveedores y usuarios del proceso, quienes podrían tener interés en consultar la información.
- Reconocer a los usuarios y beneficiarios potenciales de la información generada en el proceso.

5.6 Análisis de los activos de información y su articulación con las tablas de retención documental (TRD)

Este análisis se refiere a la identificación, calificación y valoración de los activos de información que realiza cada responsable de proceso, apoyándose en la normatividad vigente y en los criterios definidos y documentados por el Sistema de Gestión de Seguridad de la Información, como resultado de esta actividad se crea el inventario de activos de información.

Con el ánimo de optimar recursos y esfuerzos en el ICC se determina que el insumo principal para la realización del inventario de activos de información son las TRD convalidadas, así como también la identificación de los activos tipo información software, hardware, servicios e intangibles con el propósito de determinar:

- Cuáles son las series documentales y activos de información necesarios para garantizar la continuidad del negocio.
- El soporte en que se encuentra (análogo o digital).
- El propietario responsable de la información que bien puede ser un proceso, unidad administrativa, grupo de trabajo, dueños de los archivos o documentos.
- La calificación del activo de información según la Ley 1712 del 2014.
- La valoración del activo de acuerdo con los principios de confidencialidad, integridad y disponibilidad.

El ICC define que la gestión de riesgos de seguridad digital deberá priorizarse para aquellos activos cuyo nivel de criticidad en el proceso de valoración sea alto, los que se encuentren documentados en el índice de información clasificada y/o reservada y los activos que afecten de forma importante a un servicio que se preste a terceros.

5.7 Análisis de riesgos

Este es el insumo principal para la elaboración de las tablas de control de acceso y seguridad para los documentos y archivos del ICC. El análisis de riesgos se realiza únicamente para los activos de información priorizados del Instituto Caro y Cuervo, cada líder de proceso realiza la identificación de vulnerabilidades, amenazas, probabilidad de ocurrencia y nivel de impacto en el caso de una materialización del riesgo.

1) Se calcula el promedio de los valores asignados en la estimación de los activos en los principios de confidencialidad (C), integridad (I) y disponibilidad (D).
2) Se calcula de acuerdo con la frecuencia en que se hace la actividad que genera el riesgo.
3) Es la valoración dada por el usuario a nivel reputacional o económica en caso de que se materialice el riesgo.
4) Es el resultado de la probabilidad por impacto el que nos determina la zona de riesgo del activo.

5.8 Análisis de usuarios

El objetivo de realizar un análisis de usuarios es asegurar que solo los usuarios autorizados tienen acceso a los archivos y documentos, así como los permisos y restricciones. Los usuarios se clasifican en internos y externos, encontrando diferentes grupos de interés que tienen necesidades y circunstancias particulares para consultar o acceder a los archivos y documentos.

Una vez identificados los usuarios, se deben relacionar con las series y subseries documentales, de manera que la Entidad pueda implementar las acciones, requisitos y procedimientos documentados de acceso y protección de la información para cada grupo de interés.

5.9 Seguimiento y mejora

El objetivo es asegurar que las medidas de control de acceso a los documentos se cumplen de manera adecuada y que contribuyen al desempeño organizacional y la satisfacción de los requisitos y necesidades de los procesos y usuarios.

Los registros de control de acceso deben proveer la información necesaria para que en las actividades de seguimiento se pueda verificar la satisfacción de los requisitos de la Entidad y la conformidad con las políticas, procedimientos y normatividad implementada.

6 TABLAS DE CONTROL DE ACCESO (TCA)

Las Tablas de Control de Acceso (TCA) son el instrumento archivístico que permite la identificación de las condiciones de acceso y restricciones que aplican a los documentos de archivo, ya sean producidos física o electrónicamente.

6.1 Diferencia TCA y el índice de información clasificada y/o reservada

Las TCA se enfocan en proteger la información de los documentos de archivo contra el acceso, recolección, divulgación, eliminación, alteración y/o destrucción no autorizada mediante el establecimiento de unos requisitos previos para las diferentes categorías de clasificación de la información, la definición y asignación de responsabilidades de seguridad, uso y acceso a los mismos; lo cual implica una mayor cobertura frente a lo que dispone el Índice de Información Clasificada y Reservada.

De otra parte, el Índice de Información Clasificada y Reservada es el inventario de la información pública generada, obtenida, adquirida o controlada por el sujeto obligado, en calidad de tal, que ha sido calificada como clasificada o reservada; debe referirse a toda la información con que cuente una entidad, independientemente si hacen parte de documentos de archivo o no.

6.2 Calificación de la información

De acuerdo con la guía para la identificación, calificación y valoración de activos de información se establecen los criterios de calificación de la información en el Instituto Caro y Cuervo.

1. **Información pública**: información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal; ejemplo: convenios, eventos institucionales, rendición de cuentas, entre otros.

2. **Información pública clasificada**: información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. Ejemplo: Historias laborales, registros de nómina, licenciamiento de software, procesos contractuales en trámite, entre otros.

3. **Información pública reservada**: aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. Ejemplo: seguridad nacional, salud pública, relaciones internacionales, entre otros.

6.3 Permisos sobre los archivos y documentos

Los permisos se refieren a las acciones que los usuarios pueden realizar al obtener acceso a la información, son aplicables de manera independiente a cada grupo de interés o usuario interesado. Es decir, que los permisos son diferentes para cada grupo de interés o usuarios. Se proponen los siguientes permisos aplicables a los archivos y documentos:

1. Información Pública: leer, mover, copiar, distribuir y divulgar.
2. Información Clasificada (solo el personal autorizado con acceso a la información): leer, mover y copiar
3. Información Reservada (solo el personal autorizado con acceso a la información): Leer.

6.4 Formato de tabla control de acceso (TCA)

El formato de tabla tiene los siguientes campos para diligenciar:

Tabla 9 Campos para diligenciar en el formato

Campo	Descripción
Entidad productora	Corresponde al nombre de la Entidad propietaria de los archivos y documentos que son objeto de control; es decir INSTITUTO CARO Y CUERVO (ICC).
Oficina productora	Dependencia responsable de la generación, administración y custodia de los documentos quien debe ejercer el cumplimiento de las medidas de control de acceso.

Campo	Descripción
Código serie	Corresponde al código de la Serie o Subserie documental asignado en la Tabla de Retención Documental (TRD).
Serie documental	Nombre de la serie o subserie documental que es objeto de control de acceso.
Nivel de riesgo	Se determinará según el nivel de criticidad de la información, que se obtiene a partir del Índice de Información Clasificada y Reservada. El nivel de criticidad se calcula como el promedio de los valores de disponibilidad, integridad y confidencialidad (CID). El resultado de este promedio determina la clasificación de la criticidad en tres niveles: **Bajo:** Si el promedio de CID está entre 1 y 2. **Medio:** Si el promedio de CID es 3. **Alto:** Si el promedio de CID está entre 4 y 5. Este nivel de criticidad, obtenido mediante el cálculo del CID, servirá como base para determinar el Nivel de riesgo para cada serie o Subserie documental.
Tipo de usuario	Identificar el tipo de usuario que tiene acceso a los archivos de la Serie o Subserie Documental.
Grupo de Interés	Identifique el grupo de interés que tiene acceso a la información.
Detalle	Se relacionan los datos específicos de los roles o perfiles, entidades u organizaciones que pueden tener acceso a los archivos y documentos.
Permisos	Se marcan los permisos otorgados a los usuarios o grupos de interés.
Observaciones	Relacionar información acerca de precauciones, procedimientos, formatos que se deben diligenciar como evidencia de los controles de acceso implementados.

Tabla 10 Ejemplo de diligenciamiento tabla de control de acceso

	TABLAS DE CONTROL DE ACCESO (TCA)												Código: COM-F-20 Versión: 1.0 Fecha: 09/10/2024
Entidad productora			**Instituto Caro y Cuervo**									**Fecha de registro**	
Oficina productora			**Grupo de Talento Humano**									15/09/2024	
Dirección o Subdirección			**Subdirección Administrativa y Financiera**										
Código	**Serie / Subserie documental**	**Nivel de riesgo**	**Clasificación del activo**	**Tipo de usuario**	**Grupo de interés o actores relacionados**	**Permisos (Marcar con una X)**						**Observaciones**	
						Leer	**Mover**	**Copiar**	**Distribuir**	**Divulgar**	**Control total**		
10	Historias laborales	Alto	Información pública reservada	Interno	Funcionario	X						El Grupo de Talento Humano debe establecer responsabilidades	
				Externo	Entidad pública	X						Se expiden certificaciones de la información consignada en los archivos.	
Revisión	Alix Lorena Moreno Córdoba - Contratista - Oficial de seguridad de la información Jorge David Sabogal Jiménez- Coordinador Grupo de Gestión Documental												
Aprobación	Comité Institucional de Gestión y Desempeño												
Actualización	V1												

6.4.1 Revisión, aprobación y actualización

- Las tablas de control de acceso (TCA) deben ser realizadas y actualizadas por parte del coordinador de grupo y/o jefe de cada dependencia con el acompañamiento del Grupo de Gestión Documental y el Rol Oficial de Seguridad de la Información. Estas deben revisarse al menos una vez al año y actualizarse según corresponda.
- La revisión de estas, deben ser validadas por el Grupo de Gestión Documental y el Rol Oficial de Seguridad de la Información.
- La aprobación debe realizarse mediante el Comité Institucional de Gestión y Desempeño (CIGD)

6.4.2 Divulgación de las tablas de control de acceso

El Grupo de Gestión Documental es el responsable de consolidar la información y comunicar la información recolectada de los grupos de trabajo que actúan como custodios de información, además de velar porque este instrumento archivístico se mantenga actualizado y articulado con los demás instrumentos archivísticos y de la gestión pública.

7 CONCLUSIONES Y RECOMENDACIONES

Este capítulo tiene como objetivo consolidar la información presentada a lo largo de la guía incluyendo consideraciones clave para garantizar la actualización continua de estas prácticas, asegurando que la gestión documental del ICC se mantenga en cumplimiento con las normativas vigentes y responda adecuadamente a los retos futuros asignando correctamente la clasificación de la información que se produce.

Resumen de los puntos clave:

- ✓ Importancia del control de acceso: Las TCA son esenciales para asegurar la protección de la información sensible y el acceso adecuado a los documentos y archivos, tanto en formato digital como analógico.
- ✓ Cumplimiento normativo: La gestión documental del ICC está alineada con las disposiciones establecidas en el Decreto 1078 de 2015 y el Decreto 1080 de 2015, así como con los parámetros del Archivo General de la Nación (AGN) y la norma ISO 27001:2013.
- ✓ Gestión de riesgos: Se han identificado y priorizado las principales amenazas y vulnerabilidades en torno a la seguridad de la información, y se han propuesto medidas para mitigarlas eficazmente.
- ✓ Articulación con el SGSI: La integración del Sistema de Gestión de Seguridad de la Información (SGSI) en los procesos documentales es fundamental para garantizar un control efectivo y una protección adecuada de los activos de información.

Recomendaciones para la implementación:

- ✓ Actualización continua: Las TCA deben revisarse y actualizarse periódicamente, teniendo en cuenta los cambios en las normativas y en el entorno operativo del ICC. Esto incluye la incorporación de nuevos riesgos, usuarios y procesos que puedan afectar la seguridad de los documentos.
- ✓ Monitoreo y seguimiento: Se recomienda establecer mecanismos de seguimiento continuo para garantizar que las TCA y las políticas de seguridad se implementen de manera efectiva. Esto puede incluir auditorías regulares y la revisión de incidentes de seguridad.
- ✓ Capacitación: Es fundamental que el personal del ICC reciba formación constante sobre las políticas de seguridad documental y el uso adecuado de las TCA, asegurando que todos los involucrados comprendan sus responsabilidades en el manejo de la información.
- ✓ Mejora continua: A medida que el ICC enfrenta nuevos desafíos y adopta nuevas tecnologías, se sugiere que las TCA y las políticas de seguridad se ajusten para mantenerse alineadas con las mejores prácticas y normativas vigentes.

8 FORMATOS ASOCIADOS

A esta guía se asocia el formato *COM-F-20 Tablas de control de acceso (TCA)* el cual permite registrar los datos de series y subseries que produce el ICC, con el fin de clasificar la información (pública- reserva o clasificada) brindando la seguridad y el acceso a la información de la entidad. Este documento deberá ser diligenciado con acompañamiento de integrantes del proceso de Información y Comunicación.