GOB-GU-001 Guía de Aplicación de la Política de Seguridad de Trámites Físicos y Virtuales V6

TABLA DE CONTENIDO

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLA

1. OBJETIVO

Definir una guía para la aplicación de las políticas de seguridad de la información que garanticen la confidencialidad, la integridad y la disponibilidad de la información procesada en los trámites físicos y virtuales de la entidad de acuerdo con el Manual Estructura Documental – Dominio Seguridad y sus prácticas documentales del SGSI para la concesión RUNT 2.0.

2. ALCANCE

El alcance de la presente guía comprenden las directrices de seguridad en el proceso de trámites físicos y virtuales teniendo como marco de referencia las buenas prácticas de las normativas ISO/IEC 27001:2022, ISO/IEC 27002:2022, CIS Control y NIST SP800-53, los requisitos establecidos en los apéndices del contrato de Concesión 604 de 2022 del Ministerio de Transporte y sus documentos asociados articuladas bajo las “Políticas de seguridad Trámites Físicos y Virtuales” con el fin de describir los controles que representan un complemento a la efectividad los cuales permiten gestionar, definir y reglamentar la impresión, la entrega y la generación de todos los documentos resultantes de los Trámites virtuales o físicos.

3. DEFINICIONES

- **Actores:** Para el presente documento, corresponde a las entidades, organizaciones o cualquier compañía autorizada por el ministerio de Transporte a través de resolución para atender requerimientos de las personas naturales o jurídicas.

- **Especies venal:** Es todo documento, certificado o materialización del resultado de un Trámite que está asociado a un rango o serie para su propio control de expedición. (Disposiciones comunes a los apéndices)

- **Organismo de tránsito:** son aquellas unidades administrativas municipales distritales o departamentales que tienen por reglamento la función de organizar y dirigir lo relacionado con el tránsito en su respectiva jurisdicción. (RUNT)

- **Personas Jurídicas:** Es una sociedad conformada por una o más personas, capaz de ejercer derechos y contraer obligaciones, la cual puede ser representada de manera judicial o extrajudicialmente. (www.datacreditoempresas.com.co)

- **Personas Naturales:** se puede entender como aquel ser humano que desea desempeñar y ejercer obligaciones a título personal. (www.datacreditoempresas.com.co)

- **RUNT:** Sistema de información que permite registrar y mantener actualizada, centralizada, autorizada y validada la misma sobre los registros de automotores, conductores, licencias de tránsito, empresas de transporte público, infractores, accidentes de tránsito, seguros, remolques y

semirremolques, maquinaria agrícola y de construcción autopropulsada y de personas naturales o jurídicas que prestan servicio al sector. (art. 8 y 9 de la Ley 769 de 2002).

- **Trámites:** Cada uno de los pasos y diligencias que hay que recorrer en un asunto hasta su conclusión (www.rae.es).

- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente, reglas que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo[1].

- **Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.[2]

4. DESARROLLO DE LA GUIA

4.1. ÁMBITO DE APLICACIÓN

La guía de las políticas de seguridad para trámites físicos y virtuales se definen bajo las buenas prácticas normativas para la seguridad de la información como son la NTC ISO/IEC 27001:2022, por ello y frente a los aspectos de cada proceso se establecen los controles adaptados a las necesidades de la entidad.

Se debe tener en cuenta los factores que influyen dentro de las políticas para este tipo de servicios son definidas bajo las siguientes categorías incluidas dentro de la normativa de seguridad de la información:

- Controles Personas.
- Controles Tecnológicos.
- Controles Organizacionales.
- Controles Físicos.

Las políticas para cada categoría corresponderán según su tipo de tramite (Físico o Virtual). A partir de estas se articulan los controles que se contemplan dentro de la seguridad de la información y en otros casos son referenciados a las respectivas políticas y/o guías las cuales aportan más profundidad a la temática.

4.2. DOCUMENTOS ASOCIADOS

- NTC ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos GTC ISO/IEC 27002:2022

[1] gobiernodigital.mintic.gov.co - articles-150520_G2_Politica_General

[2] gobiernodigital.mintic.gov.co - articles-150520_G2_Politica_General

Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.

- CIS CONTROLS V.8. Controles para infraestructuras críticas V8.
- NIST CSF. Instituto Nacional de Estándares y Tecnología Cibersecurity Framework.
- NTC ISO/IEC 27701:2020. Ampliación de las NTC-ISO/IEC 27001:2022 y GTC-ISO/IEC 27002:2022 para la gestión de la privacidad de la información. Requisitos y directrices.
- Política de seguridad Trámites Físicos y Virtuales
- Política de Seguridad y Privacidad de la Información
- Política de Control de Acceso.
- Guía de aplicación de política de Control de Acceso.
- Guía de aplicación de política de Desarrollo Seguro.
- Política de Desarrollo Seguro.
- Política de uso de controles criptográficos.
- Guía de aplicación de política de seguridad de Blockchain
- Política de seguridad de Blockchain
- Manual estructura documental -Dominio Seguridad

Los documentos asociados son contemplados como apoyo para el aseguramiento de las actividades de trámites físicos y virtuales desde las buenas prácticas, por ello son referencias para mitigar brechas de inseguridad relacionadas con tecnologías, aplicaciones, desarrollos, controles de accesos y controles de transmisión, las cuales hacen parte del entorno de desarrollo para labores de este proceso. Estos controles representan un complemento a la efectividad los cuales permiten gestionar, definir y reglamentar la impresión, la entrega y la generación de todos los documentos resultantes de los Trámites virtuales o físicos.

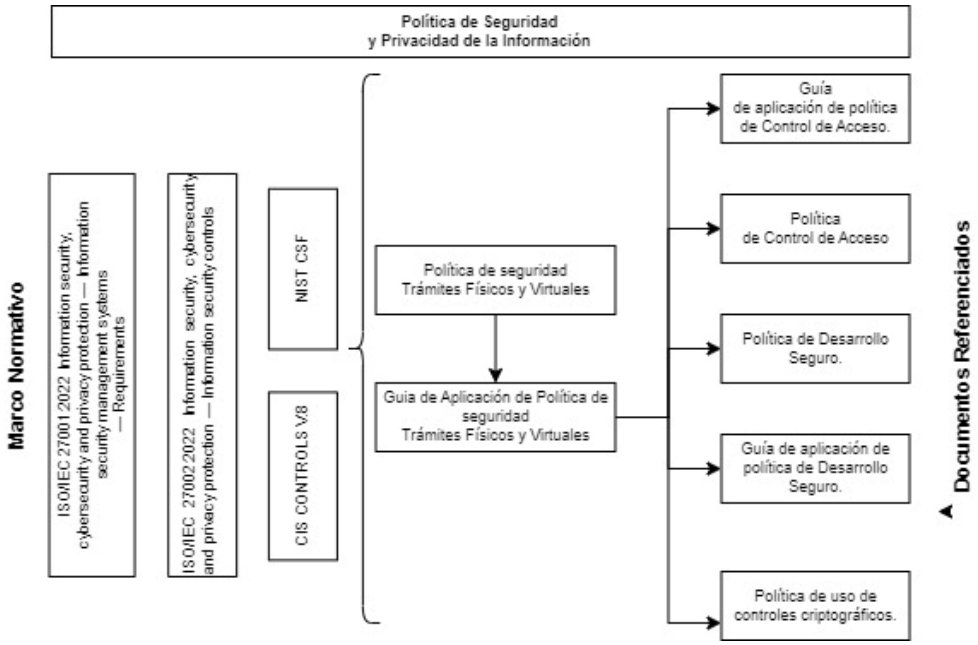

Imagen 1 Articulación controles asociados y control de trámites físicos

4.3. GUIAS GENERALES DE SEGURIDAD TRÁMITES FÍSICOS

Las generalidades desde la seguridad de la información para tener en cuenta para los trámites físico son:

- **a.** Aplicar las responsabilidades de la administración y los usuarios establecidos en la “política para el control de accesos”.
- **b.** Identificar los roles y responsabilidades de cada usuario que brinda el servicio de atención.
- **c.** Teniendo como base la clasificación de la información manejada por los responsables y según se requiera, es necesario etiquetar, controlar y tratar la información que circula por el proceso de trámites físicos.
- **d.** Capacitar a todos los responsables de los servicios de trámites físicos en normativas establecidas internamente para la seguridad de la información, aspectos legales y de comportamientos seguros para el desarrollo de sus actividades.
- **e.** Para las actividades que se desarrollen con servicios externos se establecen las cláusulas de responsabilidad y cumplimientos según los niveles de criticidad establecidos por la entidad.
- **f.** Teniendo como base la criticidad de las funciones realizadas por estos servicios, es importante contemplar las medidas de mitigación frente a eventualidades negativas que afecten la continuidad del servicio, así mismo, tener en cuenta las herramientas informáticas usadas para el desarrollo de sus actividades.

g. Las actividades realizadas bajo los sistemas de información y aplicaciones se monitorean desde el SOC según la criticidad de las responsabilidades asignadas al personal que brinda el servicio.

h. La información que requiera destrucción, anulación u otro método de desecho, tienen en cuenta los procedimientos internos establecidos para la gestión documental de la entidad.

i. La información suministrada al ciudadano o externo que requiera el servicio contempla los procedimientos internos para la divulgación y/o entrega de información bajo los niveles de clasificación.

j. La asignación de permisos y el flujo de aprobaciones para los accesos de las aplicaciones o sistemas de información se articulan con la “políticas de control de acceso”.

k. Capacitar a los responsables de trámites para que se genere conciencia de las causas de la exposición involuntaria de datos. Entre los temas de ejemplo se incluyen la entrega errónea de datos confidenciales.

4.3.1. ROLES, DEBERES Y RESPONSABILIDADES PARA TRÁMITES FÍSICOS

Los respectivos roles, deberes y responsabilidades de los actores que intervienen en el proceso de los trámites físicos ante la Concesión RUNT se detallan basados en la siguiente ilustración:

Imagen 2. Diagrama de trámites físicos.

Previo a cualquier tipo de trámite, la persona jurídica, la persona natural e incluso el vehículo al cual se expedirá el documento objeto de trámite, si a ello se refiere el trámite, debe estar inscrito o registrado y con la información y/o datos actualizados en el sistema RUNT.

A continuación, los roles existentes para los trámites físicos:

a. Persona natural o jurídica (Rol usuario solicitante)

Los usuarios solicitantes que lo requieran pueden realizar cualquier solicitud de un trámite ante los actores aprobados para tal efecto de manera presencial. Frente a su necesidad, es importante tener en cuenta que

el usuario solicitante debe suministrar los datos personales que permitan identificar y autenticar al usuario solicitante, dentro de lo cual, el ciudadano tiene la responsabilidad de autorizar el tratamiento de los datos para acceder a los diferentes servicios y trámites que requiera, ante una negativa sobre el tratamiento de los datos, el actor o responsable de gestionar el trámite, no podrá dar lugar a iniciar o resolver la solicitud ya que la gestión de los datos personales no estaría autorizada por el usuario solicitante que requiere la gestión el trámite.

b. Funcionarios, colaboradores, contratistas o empleados de los Gestores autorizados. (Rol usuarios RUNT)

Si bien los gestores autorizados y sus representantes legales son los directamente responsables de los trámites que se ofrezcan dentro de los portafolios de servicios a los usuarios solicitantes, dentro del presente esquema, se consideran partes fundamentales los funcionarios, colaboradores, contratistas o empleados de los gestores autorizados, los cuales, en cada fase o parte de los trámites que se realicen de manera presencial deberán realizar las acciones o actividades que garanticen la verificación, validación o confirmación de la información que reciban en formatos, documentos o que registren en los diferentes sistemas aprobados para almacenar la información a la que tengan acceso por ocasión de las labores encomendadas en la organización o entidad a la que se encuentren vinculados. De igual forma, es una responsabilidad fundamental, comprobar y asegurar que quien realice los trámites sea la persona correcta que presenta los documentos de identificación.

Los gestores autorizados, como sean, Organismos de Tránsito, Direcciones Territoriales de Tránsito, el Ministerio de Transporte, las academias de enseñanza, centros de reconocimiento de conductores y demás que autorizados por el Ministerio de Transporte, tengan el deber de realizar un trámite asociado a un servicio de registro, validación, modificación o expedición de un documento, deben mantener en sus instalaciones de operación y atención al cliente, la información clara, concisa y necesaria para informar y guiar a los usuarios solicitantes, ya sea persona natural o jurídica, sobre cómo y con quién proceder en sus instalaciones a realizar los trámites que requiera, por lo tanto es fundamental contar con un sistema o mecanismo guía a través de señales de orientación sobre los pasos y lugares que debe seguir para realizar la respectiva solicitud y posterior recibo de su documento o documentos resultantes. Advirtiendo en todo caso los riegos de suministrar información a personal no autorizado.

c. Sistema validador Central

El Sistema validador Central juega un papel importante en los trámites físicos, ya que a través de éstos y con la información ingresada del solicitante se procede a gestionar internamente las consultas y generación de los respectivos resultados que espera recibir la persona natural o jurídica.

4.3.2. DESCRIPCIÓN DE LAS RESPONSABILIDADES DEL ROL FRENTE A LOS TRÁMITES FISICOS

A continuación, se describe por cada Rol las responsabilidades a seguir para generar el resultado de los trámites físicos:

a. Persona natural o jurídica (Usuario solicitante)

Cuando la persona natural o jurídica realiza un trámite físico, se ejecutan los siguientes pasos:

Generación de la solicitud:

- Autenticarse a nombre propio salvo las situaciones que, por circunstancias especiales se requieran realizar mediante un poder de mandato debidamente suscrito, a cuenta y riesgo del mandante, para el trámite en cuestión.[3]
- No entregar información personal sin autorización del mandante a terceros o a otro gestor no autorizado por los organismos de control o actores oficiales encargados de gestionar los trámites.
- Suministrar datos verídicos y legítimos de contacto.
- Actualizar la información o datos que así lo requieran.
- Recibir el resultado del trámite físico ejecutado.

b. Funcionarios, colaboradores, contratistas o empleados de los Gestores autorizados. (Usuarios RUNT)

Dentro de las actividades contempladas en cada fase, se considera;

Generación de la solicitud:

El Usuario Runt que haga la recepción de las solicitudes, como gestor de estas, con la supervisión del encargado del gestor autorizado, debe:

- Verificar la identidad del solicitante mediante la comprobación visual de la persona y la presentación en físico y original de los documentos de identidad de esta. En caso de que el usuario solicitante no cuente con los documentos de identidad originales, se deberá presentar los documentos que respaldan o comprueban el documento de identidad en trámite por perdida, deterioro o robo, conforme la autoridad de Registro Civil lo autorice.[4]

- En caso de persona jurídica, verificar existencia y representación legal en el sistema RUES, contrastando esto con la documentación presentada (RUT y/o Cámara y Comercio). En caso de ser un tercero, se debe validar las autorizaciones por escrito presentadas; contrato de mandato, poder general o poder especial, a través del cual el propietario o titular confía la gestión de solicitud del trámite. Si el trámite se lleva a cabo mediante poder especial, este debe estar autenticado ante notaría pública.

[3] Artículo quinto de la Resolución No. 12379 del 28 de diciembre de 2012, expedida por el Ministerio de Transporte.

[4] Circular No. 222 del 13 de diciembre de 2016 de la registraduría nacional.

- El Usuario Runt oficial debe autenticarse con sus propias credenciales de acceso y dispositivos de autenticación asignados en los sistemas del RUNT conforme al trámite que requiera el ciudadano. Cualquier acción en los sistemas, quedará registrada como mecanismo de auditoría y por ende la responsabilidad de cualquier acción arbitraria o no autorizada sobre los sistemas de información recaerá sobre el Usuario Runt por negligencia o inobservancia.

- Cuando el trámite contemplé recategorización, se debe solicitar el documento “actual” o inicial objeto de modificación al titular de este y posteriormente una vez se entregué el nuevo documento con la nueva categoría, se debe destruir el anterior, dejando constancia ante el solicitante que este fue destruido. Esto con el fin de evitar que el documento anterior sea objeto de uso no autorizado por otro ciudadano.

- Se debe evitar almacenar de manera temporal o permanente información o datos personales en archivos, programas o repositorios de almacenamiento del equipo desde donde se registra o gestiona la solicitud.

- En las instalaciones de los gestores autorizados, se debe evitar y/o suprimir la obligación de los solicitantes de cualquier tipo de trámite en cualquier fase del proceso, de registrar información personal en planillas físicas de control que puedan resultar en documentos no controlados, esto con el fin de evitar que esta información sea hurtada para fines ilícitos u otros, y así mismo, que se atente contra la normativa de protección y privacidad de datos personales.

- Si por motivos de fuerza mayor debidamente justificados y aprobados por el representante legal del organismo de tránsito, entidad u organización autorizada para realizar trámites, se debe solicitar registro de información personal en planillas para registro y control del trámite, dicha planilla debe considerar:

    - Numero consecutivo, numerado a su vez por cantidad hojas impresas en la fecha de gestión o recopilación de datos.

    - Estar en un lugar que permita el control del registro de quienes utilizan dicha planilla.

    - Incluir en estas planillas en un campo visible y con texto de fuente completamente clara, la política de tratamiento de datos personales indicando principalmente que, al registrar la información personal en dicha planilla, el usuario acepta el tratamiento de sus datos personales allí solicitados bajo las consideraciones de la norma vigente,

    - Al finalizar el día, el encargado en la entidad u organización gestora del trámite deberá consolidar y validar que las planillas estén completas y no hayan sido afectadas en su integridad, afectando los datos registrados. En caso de que se evidencie perdida o daño severo de alguna de estas, se deberá realizar el debido proceso como un incidente de seguridad de la información y tomar las medidas disciplinarias o legales que correspondan.

- Dichos documentos deben ser resguardados en un lugar seguro con controles de acceso y consulta debidamente normados y auditados.

- No permitir que una persona o conjunto de personas ajenas a la organización visualice, grabe o tome notas de la información y/o datos que se manejen durante cualquier fase del trámite. Por lo tanto, ante la necesidad de registro de información en planillas, un colaborador del gestor del trámite siempre debe estar presente en el momento en el que los usuarios realicen el diligenciamiento de los datos.

- Se debe notificar a las autoridades sobre cualquier indicio de posible suplantación de personas o intento de robo de datos personales evidenciados en los procesos de registro de solicitudes o gestión de trámites.

- Realizar las gestiones a que haya lugar para culminar el proceso de generación, impresión y entrega del documento resultado del trámite, procurando garantizar en cada fase, la confidencialidad, la integridad y disponibilidad inmediata de los documentos y datos asociados al mismo y al(los) titular(es), sea persona jurídica o personal natural.

- Resguardar, conservar y proteger las credenciales de acceso y dispositivos de autenticación de los sistemas y aplicaciones de RUNT u otros que les haya sido asignados, ante usos por parte de personal no autorizado. Al respecto se debe implementar lineamientos de obligatorio cumplimiento como:

  - Una vez finalizada la jornada laboral, almacenar los tokens de autenticación en un lugar seguro, resguardado y en lo posible cerca a los circuitos cerrados de vigilancia y control.

  - Si se decide portar en todo momento el token o dispositivo de autenticación, ante la posibilidad de pérdida o robo, se debe reportar inmediatamente al representante legal del gestor autorizado y a su vez a la concesión RUNT mediante el canal de solicitudes dispuesto, con el fin de iniciar el trámite de revocación.

- Reportar inmediatamente la identificación de vulneración de accesos con sus credenciales y/o dispositivos de autenticación ante el representante legal del gestor autorizado para iniciar las actividades de reporte a las autorizadas o encargados de investigación y/o denuncia a las autoridades con el fin de realizar una correcta gestión de incidentes de seguridad de la información. Y de igual forma, reportar a RUNT para gestión auditoría e inactivación o cambio de credenciales de los accesos concedidos.

Impresión y entrega del documento resultado del trámite:

El funcionario, colaborador o empleado que realice la impresión del(los) documento(s) resultado del trámite requerido por la persona natural o jurídica, debe:

- Si el documento que entrega al solicitante corresponde a la impresión de un formato generado por el sistema RUNT, este deberá ser impreso en el momento en que el solicitante se presente presencialmente a recibirlo.

- La impresión del documento, en caso de ser resultado de un formato del sistema RUNT, realizada en las instalaciones de un actor (gestor del trámite), debe llevar impresa la fecha y hora de impresión, nombre de quien imprime (usuario del sistema) y nombre host (nombre del equipo), esto impreso en uno de los bordes del documento.

- No se debe conservar en el almacenamiento local de los equipos de cómputo ni en medios de almacenamiento removibles, copia de ningún documento generado en la gestión de un trámite. El gestor autorizado, debe realizar revisiones periódicas de que esto se cumpla.

- Tanto la entrega como la recepción del documento, en tanto ocurran en una instalación física del gestor autorizado, debe ser firmado ya sea física o digitalmente por quien lo entrega (funcionario, colaborador o empleado de actor que gestiona) y por quien lo recibe (persona natural, jurídica o delegado autorizado de alguna estas), incluyendo dentro de los campos para tal fin, la fecha y hora en que se realiza este paso.

- Cuando los documentos a entregar correspondan a trámites de tipo especie venal, es decir, entrega de documentos en formato “plástico” como son; licencias, tarjetas de registro o permisos, la impresión en cada fase que competa debe atenerse obligatoriamente a la normativa que se defina para tal efecto, tanto para la numeración del documento por cada una de las partes intervinientes en su fabricación y tratamiento, como para el tipo de impresión, forma y estructura final.

- Se debe siempre comprobar y validar que quien realiza, genera o desencadena el trámite sea quien reciba el documento, en todo caso, no se deberá hacer entrega o envío del documento resultado del trámite a una persona diferente al solicitante o autorizado por el solicitante para tal efecto.

c. Sistema(s) de información y/o registro

Los sistemas de información y/o registro de información, deben:

Generación de la solicitud:

- En caso de que el usuario solicitante presente documento de identidad original no definitivo, es decir, certificado de documento en trámite, de acuerdo con lo autorizado por Registraduría Nacional, el sistema debe contar con un control tipo check que permita registrar dicha situación.

- Asignar un número único y específico para cada trámite solicitado.

- Asignar un código único y específico a los documentos que se imprimen, como resultado de la solicitud realizada por el usuario solicitante.

- A través de la codificación, el sistema debe permitir por cierto tiempo, consultar el documento resultado de manera digital. En todo caso, el sistema debe almacenar un registro del resultado del trámite con el identificador del documento generado resultado del trámite y la especificación de que si este fue impreso en un organismo de tránsito o actor que gestiona o en su defecto indicar que no fue impreso si no enviado digitalmente.

Impresión y entrega del documento resultado del trámite:

- El sistema debe ser parametrizado y/o desarrollado para almacenar un registro inicial de la fecha y hora tanto de la generación, como de la descarga del documento resultado del trámite y con posteridad, los registros que indiquen la fecha y hora que fue descargado el documento con la correspondiente información de qué usuario realizó la descarga, solo si esto tratase de un usuario autorizado de un organismo de tránsito u otro actor con acceso.

- El sistema debe almacenar de manera indefinida la fecha y hora de generación del documento, nombres y/o usuarios en sistema de quienes intervinieron en la gestión y entrega del documento resultado del trámite y así mismo, registro de recepción del documento, por parte de la persona natural o jurídica quien generó el trámite y recibe el documento solicitado.

- El sistema debe ser parametrizado de tal forma que permita registrar la recepción a satisfacción de los documentos resultados de los trámites, a través de mecanismos de autenticación biométrica, garantizando la seguridad del registro a través del cifrado de los datos. Estos registros deben quedar registrados con estampas de tiempo basadas no en la hora local de los sistemas si no de la hora del servidor donde opera el software o aplicación con la cual se registra y hace seguimiento al trámite.

- Se deben implementar mecanismos que permitan validar la autenticidad del documento impreso.

4.4. GUIAS GENERALES DE SEGURIDAD TRÁMITES VIRTUALES

Las generalidades desde la seguridad de la información para tener en cuenta para los trámites virtuales son:

a. Una vez al año establecer pruebas de vulnerabilidades para las aplicaciones dispuestas para los servicios de trámites virtuales, estos deben tener en cuenta las disposiciones de seguridad definidas en las “Políticas de desarrollo seguro”.

b. Remediar las vulnerabilidades de las aplicaciones bajo los procesos de evaluación previamente realizados y según la frecuencia establecida. Se deben establecer categorización de vulnerabilidades estableciendo grados de criticidad para estas.

c. Disponer de plataformas con los versionamientos actualizados, estos deben comprender las aplicaciones o sistemas de información, bases de datos y otras arquitecturas que hagan parte de los trámites virtuales.

d. Generar evidencias de responsabilidades por parte de los usuarios para la información que se ingresa a aplicaciones o sistemas de información virtuales.

e. Contemplar las normativas y aspectos legales frente a la información solicitada en los procesos de diligenciamiento de información bajo los trámites virtuales.

f. La selección y/o diseño de aplicaciones o sistemas de información para la prestación de los servicios virtuales se articulan con las buenas prácticas de los lineamientos establecidos para el desarrollo de seguro.

g. Los servicios virtuales dispuestos para la atención de las personas jurídicas o naturales no deben permitir utilizar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.

h. Contemplar el aseguramiento de las plataformas dispuestas para el servicio bajo conceptos de buenas prácticas un ejemplo podría ser “seguridad en capas – Seguridad en profundidad”.

i. Las actividades de impresión se establecerán bajo un rol de acceso especifico “Perfil” para las aplicaciones y/o Sistemas de Información que limite las acciones del usuario relacionados con las impresiones de especies venales y formatos.

j. Los servicios virtuales dispondrán de un canal cifrado en la transmisión de los datos de los titulares y/o información sensible.

k. Se debe controlar el acceso a la información que se dispondrá para el ejercicio de atención física por parte de los funcionarios, contratistas y/o responsables de la actividad, para ello deben ser establecidos los permisos bajo el principio del “mínimo privilegio”. Solo se dispondrá los permisos requeridos para el cumplimiento de sus funciones.

l. Periódicamente y no mayor a tres meses, realizar la validación de privilegios y usuarios de acceso para los funcionarios, o responsables de brindar el servicio de atención frente a los sistemas de información o aplicaciones dispuesta para el desarrollo de sus labores.

m. Establecer para los sistemas de información o aplicaciones perfiles de acceso preestablecidos como base de asignación a los servicios informáticos.

n. Realizar monitoreos y generación de alertas para los comportamientos de acceso a los recursos virtuales, teniendo en cuenta los “análisis de comportamientos”, de ser posible el establecimiento de “inteligencia de eventos”.

o. Capacitar o establecer campañas a los usuarios de los servicios virtuales en la conexión y transmisión de datos a través de redes inseguras para actividades empresariales.

p. Contemplar aquellos controles que permitan las funciones automatizadas, como referencia se pueden tener en cuenta los controles definidos en la NIST SP800-53.

4.4.1. ROLES, DEBERES Y RESPONSABILIDADES PARA TRÁMITES VIRTUALES

Los respectivos roles, deberes y responsabilidades de los actores que intervienen en el proceso de los trámites virtuales ante la Concesión RUNT se detallan basados en la siguiente ilustración:

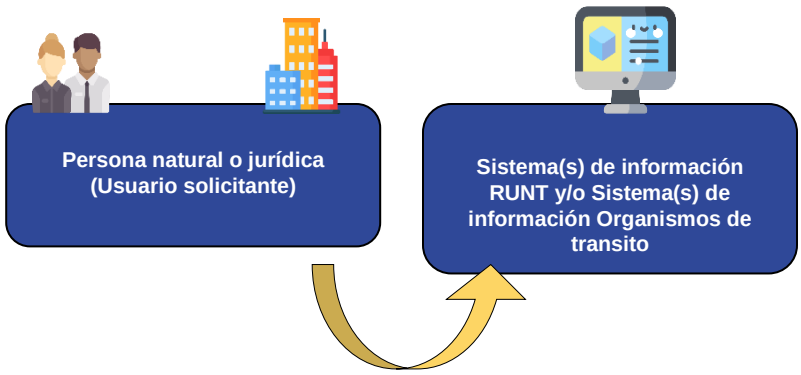

Imagen 3. Diagrama de trámites virtuales.

Para los trámites que realizan de manera virtual, los cuales se llevan a cabo a través de un equipo de cómputo con conexión a internet o los sistemas de información de los Organismos de tránsito los cuales tienen interoperabilidad con los SI del RUNT, para ello, se establecen básicamente dos (02) intervinientes, el usuario solicitante, como desencadenador, quien puede llegar a ser una persona natural o jurídica la cual previamente debe realizar un registro en la plataforma o sistemas de información (Validar Central - RUNT y/o Organismo de tránsito) donde se realiza la consulta o generación de documentos y por otro lado, el sistema de información, el cual actúa de manera programada y automática para confirmar titularidad de los datos registrados y presentar los formularios de solicitud de datos e información habilitados como requisitos para resolver o generar el documento resultado del trámite.

Considerando que, para este tipo de trámites, no existe un encargado de validar, confirmar y autorizar los trámites solicitados a través de los sistemas de información dispuestos para tal fin, a continuación, se describen las condiciones en las que se orquestan este tipo de requerimientos con base en las responsabilidades de quienes los administran o son.

a. Persona natural o jurídica (Usuario solicitante).

Previo a cualquier tipo de trámite, la persona jurídica, la persona natural e incluso el vehículo al cual se expedirá el documento objeto de trámite, si a ello se refiere el trámite, debe estar inscrito o registrado y con la información y/o datos actualizados en el sistema RUNT o cualquier otro con el que se interactúe y que esté dispuesto por la Concesión RUNT 2.0 para gestionar de manera digital la resolución de un trámite que genera o envía un documento que en fin cumplirá con las mismas condiciones de legalidad que el documento físico.

Para algunos trámites, los usuarios solicitantes pueden realizar el requerimiento de generación de documentos de manera virtual a través de los canales digitales dispuestos para ello en el sitio WEB de la Organización. No obstante, para hacer uso de estos servicios digitales, se debe cumplir una serie de

requisitos previos con el fin de que el sistema, que esta previamente programado para recibir unos datos, pueda dar lugar a generar los documentos requeridos.

Es importante tener en cuenta que el usuario solicitante suministre los datos personales que permitan validar la titularidad de su información registrada para usar el sistema de información facilitador del trámite, dentro de lo cual, el usuario solicitante tiene la responsabilidad de autorizar el tratamiento de los datos personales que suministre. Ante una negativa sobre el tratamiento de los datos, el sistema de información o aplicación facilitadora no podrá dar lugar a iniciar o realizar dicha solicitud ya que la gestión de los datos personales no estaría autorizada por el usuario solicitante que requiere la gestión el trámite.

Se deben implementar mecanismos de autenticación de la identidad de la persona que esta originado el trámite en función de la criticidad del trámite.

b. Sistema(s) de información y/o registro o Sistema(s) de información Organismos de transito

Los sistemas de información y/o registros (validar central) o Sistemas de información de organismos de tránsito juegan un papel importante en los trámites físicos, ya que a través de éstos y con la información ingresada del solicitante se procede a gestionar internamente las consultas y generación de los respectivos resultados que espera recibir la persona natural o jurídica.

4.4.2. DESCRIPCIÓN DE LOS DEBERES POR CADA ROL EN TRÁMITES VIRTUALES

A continuación, se describe por cada Rol los pasos a seguir para generar el resultado de los trámites físicos:

c. Persona natural o jurídica (Usuario solicitante).

Generación de la solicitud:

- Autenticarse a nombre propio o de la persona jurídica a la que representa y la cual cedió de manera explícita los derechos de gestionar los trámites en los sistemas de información habilitados.
- Validar y confirmar que se está realizando el registro de información en un sistema o aplicación legítimo, en todo caso el usuario es responsable del uso de los sistemas y aplicaciones y el registro de su información personal.
- Suministrar datos verídicos y legítimos de contacto.
- Suministrar información legitima, clara y legible cuando así lo requiera el sistema de información.
- Actualizar la información o datos que así lo requieran.

Impresión y entrega del documento resultado del trámite:

- El usuario es libre de elegir si el documento resultado del trámite es impreso o no, en todo caso, la impresión del documento generado y su control es responsabilidad única del usuario que lo generó e imprimió.

d. Sistema(s) de información y/o registro

Los sistemas de información y/o registro de información, deben:

Generación de la solicitud:

- Proveer un servicio de validación de registro que corrobore la titularidad del usuario registrado, mediante correo electrónico.

- En los casos y sobre las plataformas desde donde se realice el registro, realizar validaciones de legalidad de los documentos de identidad comprobantes del registro y así mismo realizar validaciones biométricas, si es posible que quien realiza el registro coincide con el titular de los datos.

- Transmitir entre el cliente y el servidor la información de manera cifrada, es decir, proveer un mecanismo de comunicación seguro.

- Evitar y no permitir que se registren los mismos datos de identificación o contacto en diferentes cuentas.

- Garantizar que la autorización de acceso al sistema o aplicación se realizó de manera legítima, establecimiento controles de acceso mediante usuario, contraseña y en casos especiales mecanismos de autenticación adicionales como segundo factor de autenticación entre otros.

- Asignar un número único para cada requerimiento de información.

- Asignar un código único a los documentos generados como resultado de los trámites.

- Los documentos generados deben ser firmados digitalmente de manera que se pueda verificar la autenticidad de la información contenida.

- A través de la codificación, el sistema debe permitir por cierto tiempo, consultar el documento resultado de manera digital. En todo caso, el sistema debe almacenar un registro del resultado del trámite con el identificador del documento generado.

Impresión y entrega del documento resultado del trámite:

- El sistema debe ser parametrizado y/o desarrollado para almacenar el registro inicial de la fecha y hora de la generación del documento resultado del trámite.

- El sistema debe almacenar de manera indefinida la fecha y hora de generación del documento, nombres y/o usuarios en sistema de quienes intervinieron en la gestión y/o envío del documento resultado del trámite y así mismo, registro de aceptación del documento, por parte de la persona natural o jurídica quien generó el trámite y recibe el documento solicitado.

- Permitir la consulta mediante el identificador único asignado al documento resultado del trámite, como un servicio de comprobación asociada al sistema de información, para validar la legalidad del documento gestionado.

4.5. CONTROLES DE SEGURIDAD PARA LOS TRÁMITES FISICOS Y VIRTUALES.

Se contemplan bajo este tipo de trámites los controles relacionados en las normas NTC ISO/IEC 27001:2022, sin embargo, es importante tener claridad que lo propuesto comprende los controles referenciados y adaptados a los procesos de trámites físicos y virtuales. Las categorías que se tienen en cuenta para los controles son:

- Controles Personas.
- Controles Tecnológicos.
- Controles Organizacionales.
- Controles Físicos.

Teniendo como base las políticas establecidas se procede con el establecimiento de los controles que se dispondrán para el contexto de seguridad de la información de estos dos tipos de trámites, en ese orden se establecen disposiciones de seguridad teniendo como base los siguientes controles:

Controles personas:

- Contar con acuerdo de confidencialidad o no divulgación para la información crítica de las actividades de trámites, estos deben ser establecidos bajo las normas legales, y contractuales para los usuarios internos del RUNT del proceso de trámites de la Concesión RUNT 2.0.

- Garantizar que los usuarios externos conozcan las responsabilidades de la entidad frente a la información cargada en los sistemas de información, también se debe exponer las implicaciones legales frente a la veracidad de esta.

- Establecer procesos de formación, capacitación y/o difusión de los peligros de conexiones inseguras para las actividades de trámites bajo las aplicaciones dispuestas para el servicio. Se contemplan los siguientes temas:

    - Conexión en sitios públicos.

    - Responsabilidades en el uso de las aplicaciones.

- Riesgos frente a las practicas inseguras en la creación de contraseñas.
- Responsabilidades en el uso de la información de la entidad entre otras.

Controles tecnológicos:

- Establecer frecuencias de revisión de vulnerabilidades para los activos de información establecidos como críticos usados para los servicios de trámites físicos y virtuales; se debe contemplar los riesgos del entorno y las directrices de seguridad de la información establecidas por la entidad y deben ser realizadas al menos una vez al año. Las pruebas realizadas se deben socializar y gestionar su remediación de acuerdo con los procedimientos establecidos en la entidad Concesión RUNT 2.0.

- Las aplicaciones o sistemas de información deben contar con sus parches (actualizaciones) respectivas, las brechas de seguridad se cerrarán posterior a la evaluación y remediación de las vulnerabilidades.

- La infraestructura TI de la concesión RUNT 2.0 del proceso de tramites físicos y virtuales contaran con un programa de actualización e inclusión de medidas de protección antivirus, endpoint u otras herramientas.

- Los desarrollos, adquisiciones para las aplicaciones y/o sistemas de información para los servicios virtuales contemplan las condiciones establecidas en la "Política de desarrollo seguro" del SGSI de la Concesión RUNT 2.0.

- Con el fin de garantizar la confianza de los usuarios externos para las aplicaciones de los servicios virtuales, se tendrán en cuenta para la seguridad de las conexiones y sistemas de información:
  - Certificados TLS para los sistemas de información.
  - Roles preestablecidos para los sistemas de información.
  - Aseguramiento de comunicaciones por medio de VPN's.
  - Factores de autenticación adicionales a la contraseña.
  - Códigos de validación frente a posibles bots (Captcha).
- Desde el monitoreo de seguridad es importante establecer alertas a los comportamientos de acceso frente a las actividades realizadas por los usuarios de las aplicaciones de trámites; los accesos externos deben establecer comportamientos bajo el concepto "Inteligencia de amenazas" de la norma NTC ISO/IEC 27001:2022, entre las que se encuentra el accionar proactivo ante amenazas y posible materialización de incidentes.

- La entidad debe contemplar con el apoyo del área de TI la implementación de tecnologías de autenticación que permitan disponer a los usuarios de las aplicaciones y/o sistemas de información un nivel adicional de seguridad, se deben tener presente:
  - Métodos de autenticación como lo son SSO (Single Sign on), protocolos SAML y WS-FEDERATION, OPEN ID CONNECT (OIDC), AD/LDAP entre otros.

- Factores de autenticación como podría ser el caso de los PINES, Dispositivos fuera de banda, Dispositivo OTP factor único y Dispositivos OTP multifactor.

- Como medida de seguridad adicional para los accesos a los sistemas de información / aplicaciones se deberían contemplar el múltiple factor de autenticación como método de autenticación para verificar la identidad de un usuario para un inicio de sesión u otra transacción (NIST SP 800-53, IA-2(6)).

- Las aplicaciones deberían finalizar automáticamente una vez se cumplan los tiempos de espera predefinidos u otros eventos que desencadenen el cierre inmediato de la aplicación (NIST SP 800-53, AC-12).

- Se sugiere que frente a la terminación de sesión se presenten mensajes de notificación de finalización o de continuación de sesión (NIST SP 800-53, AC-12(3)).

- Una vez caducado los certificados digitales, se debe proceder con la destrucción de los mismos, de tal manera que este no pueda ser reconstruido (mínimo 2 partes); la disposición final de estos dispositivos electrónicos debe ser separada.

- Al terminar la relación laboral con la entidad, se debe asegurar que se revoquen los certificados digitales ante el ente certificador; así mismo, se deben cancelar las credenciales de acceso a los sistemas de información.

Controles organizacionales:

- Los requisitos legales, reglamentarios y contractuales serán identificados por los actores de los trámites físicos y virtuales, con ello se generar conciencia y establecerá responsabilidad frente al manejo de la información que se carga en las aplicaciones y/o sistemas de información.

- Las aplicaciones usadas para el desarrollo de las actividades de trámites deben contar con un inventario de aplicaciones, roles, responsabilidades y permisos. Es importante según las restricciones de acceso se establezcan alcances para los distintos permisos teniendo en cuenta la clasificación de la información realizada bajo el SGSI de la entidad. Se debe tener en cuenta:

  - Los activos de información y sus niveles de clasificación, esto conlleva a identificar la criticidad de esta desde regulaciones y otros aspectos que sean del ámbito y alcance de la concesión RUNT 2.0 así como las medidas para tener en cuenta durante su uso, por ejemplo “Datos Personales”.

  - Nivel de confidencialidad de la información.

  - Controles de estos para su acceso etiquetado y entrega.

- Diseñar medidas de contingencia en conjunto con la gestión de continuidad para los eventos de interrupción o de afectación al servicio de trámites por parte de la entidad y de frente a los usuarios. Se deben contemplar aspectos como:

  - Recursos humanos de la operación del servicio.

  - Continuidad de los procesos realizados frente a los escenarios identificados durante las interrupciones.

- Tiempo de ejecución de los planes de restablecimiento de las actividades.

- Establecer desde las buenas prácticas parámetros de seguridad que permitan la creación contraseñas fuertes para los accesos a los sistemas de información de los trámites. Estas obligaran al uso de más de 8 caracteres, así como números y caracteres especiales o según lo defina la entidad.

- El responsable de tramites en conjunto con el oficial de seguridad de la información debe realizar el seguimiento del cumplimiento y la eficacia de los controles definidos bajo la presente guía. Para tal fin; se definen los siguientes criterios para la evaluación de la eficacia del control deben responder las siguientes preguntas.

  - Tipo de control (Preventivo, Detectivo, Correctivo).
  - ¿Tiene un responsable definido? (Si-No).
  - ¿Su ejecución es sistematizada o manual? (Automática – Manual).
  - ¿Cuál es la periodicidad de la aplicación del control? (Continua, Diaria, Mensual, Trimestral etc.).
  - ¿Se tiene evidencia de la aplicación del control? (Si-No).
  - ¿Se encuentra documentado él control? (Si-No).

Controles Físicos:

- Los responsables de las áreas restringidas y los encargados del manejo y custodia de los activos de información deben realizar al menos una revisión anual (o cuando sea requerido) sobre los derechos de acceso de los usuarios autorizados en intervalos regulares, con el fin de mantener un control eficaz de acceso a los datos e información y a los servicios de información que ofrecen los sistemas de información, aplicaciones y/o bases de datos.

- Es responsabilidad de la Gerencia de Infraestructura de TI y Seguridad Física la definición de los controles biométricos, así como los respectivos accesos a espacios de uso restringido y verificar los permisos a través de las respectivas tarjetas de proximidad y garantizar el almacenamiento del registro a cada una de las áreas de la Concesión RUNT 2.0. en donde se evidencie quien ingresa con fecha y hora a los recintos de ésta.

5. CONTROL DE CAMBIOS

Control de cambios					
Versión	**Elaboró**	**Revisó**	**Aprobó**	**Fecha**	**Descripción**
1	IT Managers	Jefe de Seguridad de la información	Líder de Dominio de Seguridad	22/11/2022	Elaboración Inicial
2	IT Managers	Jefe de Seguridad de la información	Líder de Dominio de Seguridad	05/12/2022	Ajustes realizados por revisión de interventoría “RUNT2-DA-M03-F01- GOB-PT-003 Política Trámites Físicos y Virtuales V2”
3	IT Managers	Jefe de Seguridad de la información	Líder de Dominio de Seguridad	20/01/2023	Ajustes realizados por revisión de interventoría “RUNT2-DA-M03-F01- GOB-GU-001 Guía de aplicación de política de Tramites físicos y Virtuales V3”

4	IT Managers	Jefe de Seguridad de la información	Líder de Dominio de Seguridad	09/02/2023	Ajustes realizados por revisión de interventoría “RUNT2-DA-M03-F01- GOB-GU-001 Guía de aplicación de política de Tramites físicos y Virtuales V3”
5	IT Managers	Jefe de Seguridad de la información	Líder de Dominio de Seguridad	23/02/2023	Ajustes realizados por revisión de interventoría “RUNT2-DA-M03-F01- GOB-GU-001 Guía de aplicación de política de Tramites físicos y Virtuales
6	IT Managers	Jefe de Seguridad de la información	Líder de Dominio de Seguridad	17/03/2023	Se ajusta la palabra Transporte en el documento.

Tabla 1 Control de cambios