MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DEPARTAMENTO: Administrativo

PROCESO: Tecnologías de información

CONDICIÓN:	Actualizado
VERSION:	007

ELABORADO POR:	**PROCESO DE TECNOLOGÍAS DE INFORMACIÓN**
	Ronald Vargas Bermúdez Encargado de Proceso de Tecnologías de Información

	Sesión	**Acuerdo**	**Fecha**
APROBACIÓN: (Por el órgano Colegiado)	Ordinaria 44-2021	TRA-SE-157-2021	23 de setiembre de 2021

TABLA DE CONTENIDO

CONTROL DE VERSIONES Y CAMBIOS.

Número de versión	Fecha de aprobación	Sesión en que se aprueba	Acuerdo de aprobación	Razón del cambio
001	01 de Julio de 2015	Ordinaria 26-2015	TRA-SE-883-2015	Procedimiento inicial
002	22 de noviembre de 2017	Ordinaria 45-2017	TRA-SE-423-2017	Se actualiza el documento en cuanto al fondo y formato con la asesoría de PricePWC.
003	01 de noviembre de 2018	Ordinaria 42-2018	TRA-SE-396-2018	Se actualiza la política #4 inciso 9
004	06 de diciembre de 2018	Ordinaria 47-2018	TRA-SE-420-2018	Se actualiza la política #6 inciso 9 y 10.
005	14 de febrero de 2019	Ordinaria 06-2019	TRA-SE-044-2019	Se cambia el formato y el nombre por estandarización de normativa interna el nombre del documento de Marco de Políticas de Seguridad de la Información a Políticas de Seguridad de TI
006	03 de setiembre de 2020	Ordinaria 41-2020	TRA-SE-151-2020	Se realiza actualización acorde a la nueva normativa TIC.
007	23 de setiembre de 2021	Ordinaria 44-2021	TRA-SE-157-2021	Se incorpora Nomenclatura para asignar nombre de equipo de cómputo en el *artículo 14*. Además, se modifica

				el artículo 36: Política de seguridad de la información para las relaciones con proveedores, para una mejor definición del procedimiento.

RESPONSABLE DE ACTUALIZACION

Ronald Vargas Bermúdez, Encargado Proceso de Tecnologías de Información

DEFINICIONES

Criptografía: en el contexto de este documento debe entenderse como el conjunto de artefactos que facilitan la implantación de mecanismos, protocolos y sistemas que se utilizan para la seguridad de las comunicaciones y el acceso e intercambio de información entre entidades en términos de preservar la confidencialidad y la integridad de dicha información.

Dueños de servicios e información: jefaturas o encargados de procesos institucionales que ejercen la representación de la institución como dueña de la información; son los responsables de estos procesos ante la administración.

Información sensible: Para efectos de esta política, se entenderá como datos e información sensible, la siguiente:

- Información personal sensible e Información de Identificación Personal: De conformidad con la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, los datos personales de acceso restringido que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública; son muy sensibles. En este sentido, será considerada sensible la información gestionada por el TRA en las resoluciones, específicamente la dirección exacta de las personas físicas.
- Datos sensibles que gestiona el TRA respecto de los funcionarios, específicamente la dirección exacta de sus domicilios, los salarios exactos y algunos datos que constan en los expedientes personales; estos datos no se divulgan a la ciudadanía sino a las instituciones que requieren la información.
- Datos relativos a la configuración o a las tecnologías de los sistemas informáticos del TRA.

- Datos detallados relacionados con registros de acceso o actividad de una persona (tanto usuarios internos como externos) disponibles en los sistemas informáticos del TRA.
- Los datos proporcionados al TRA por otra organización pública o cualquier otro organismo con el cual se haya firmado un memorando de entendimiento o un acuerdo de no divulgación se considerarán datos confidenciales.
- Datos transaccionales detallados de terceros: Los datos transaccionales detallados de terceros contenidos en documentos individuales o en las bases de datos transaccionales como producto del ejercicio de la actividad o competencia del TRA. En esta categoría se incluyen los datos que envía el TRA a las diferentes instituciones gubernamentales como la CCSS, INS, Tesorería Nacional.

Riesgo: Posibilidad de que ocurran eventos que tendrían consecuencias, positivas o negativas, sobre el desarrollo de la gestión institucional, afectando el cumplimiento de los objetivos fijados. Específicamente en esta categoría deberán ser considerados todos aquello "eventos originados por el manejo inadecuado u omiso de la comunicación interna o externa, la gestión documental física o digital o las tecnologías de información."

Persona usuaria: Es un individuo que está autorizado a acceder a activos de información del TRA, de acuerdo con sus funciones y responsabilidades. Es la persona autorizada para acceder a los activos de información; estas personas usuarias tienen un rol crítico en el esfuerzo de proteger y mantener la información de la Institución. Para propósitos de seguridad de la información, las personas usuarias de los activos de información pueden ser personal permanente o temporal.

Servicio de TI: Un servicio es considerado aquel medio que entrega valor al cliente o persona usuaria, facilitándole los resultados en la operación y por ende en la consecución de sus

objetivos. Para efectos de este documento, el cliente del servicio serán todas aquellas áreas, departamentos o áreas usuarias dueñas de la información y de los servicios; y éstos serán provistos por un proveedor, en este caso la dependencia encargada de la Gestión de las Tecnologías de Información. De manera que se establezca una relación de proveedor-cliente.

Sistema de detección y prevención de intrusiones (Intrusion Prevention/Detection System, IPS/IDS por sus siglas en inglés): es un programa de detección y/o prevención de los accesos no autorizados a un computador o a una red.

Terceros: Cualquier persona física o jurídica o sujetos interesados ajenos a la Institución, por lo general son proveedores y otras entidades con las que el TRA requiera intercambiar información.

Tecnologías de Información: definidas como el conjunto de técnicas para la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos institucionales, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella, de una forma eficaz, eficiente y económica, y con apego al bloque de legalidad. Incluye elementos de hardware, software, telecomunicaciones y conectividad, entre otros.

INTRODUCCIÓN

La información es un activo que, como el resto de los activos, tiene un valor muy importante para el Tribunal Registral Administrativo (en adelante, TRA) y por esta razón, debe ser protegida de la mejor manera posible, minimizando los riesgos de daño y contribuyendo de esta forma a una mejor gestión del TRA.

Con tal de proteger esta información y en cumplimiento de Política General de Seguridad de la Información y en cumplimiento a los objetivos de seguridad de la información definidos en dicha política, se ha generado este documento que contiene los lineamientos específicos para la gestión de la seguridad de la información institucional agrupadas por dominio específico.

El presente manual cubre los siguientes dominios de seguridad de la información:

1. Gestión sobre las políticas de seguridad de la Información
2. Organización de seguridad de la Información
3. Seguridad de los Recursos Humanos
4. Gestión de Activos
5. Control de Acceso
6. Seguridad Física y Ambiental
7. Cifrado
8. Seguridad de las operaciones
9. Seguridad de las comunicaciones
10. Adquisición, desarrollo y mantenimiento de sistemas
11. Relaciones con los proveedores
12. Gestión de incidentes de seguridad de la información
13. Cumplimiento

Una de estas políticas, incluye la estructura de responsabilidades para la gestión de la seguridad cuyo enfoque para la protección de activos de información y de valor de la organización, es integral; en otras palabras, abarca a todo el personal del TRA. Esto aunado a la pluralidad de habilitadores que intervienen en el proceso, hacen necesaria la intervención y compromiso de distintas interesadas iniciando desde la Alta Administración.

TITULO I:
GESTIÓN SOBRE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Artículo No. 1: Políticas de seguridad de la información

El manual de políticas de seguridad de la información vigente será actualizado por el rol que la Administración haya asignado como encargado de Seguridad de la Información, quien lo presentará al Comité del Tecnologías de Información para su revisión. Las aprobaciones finales serán realizadas por el Órgano Colegiado.

a. La dependencia encargada Proceso de Tecnologías de Información y el rol encargado de la Seguridad de la Información, realizarán las gestiones requeridas para que el manual de políticas de seguridad de la información o las políticas de dominio específico contenidas en él, sean comunicadas a todos los funcionarios del TRA.
b. El Comité del Tecnologías de Información deberá revisar y actualizar las políticas de seguridad de la información contenidas en el presente documento una vez al año o cuando los cambios en el entorno lo exijan.
c. El Órgano Colegiado podrá ordenar revisiones y auditorías al proceso general de Seguridad de la Información, tal cual se contempla en los diferentes dominios de seguridad cubiertos en el presente manual.

TITULO II
ORGANIZACIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN INSTITUCIONAL

Artículo No. 2. Estructura organizacional para la gestión de la seguridad de la información.

Para una correcta implementación de esta política de gestión de la seguridad de la información, es necesario contar con una estructura organizacional que permita asumir los diferentes roles y responsabilidades. El TRA debe definir y mantener un esquema de seguridad de la información en donde existan roles y responsabilidades que consideren actividades de administración, operación y gestión de la seguridad de la información, mismo que detalla:

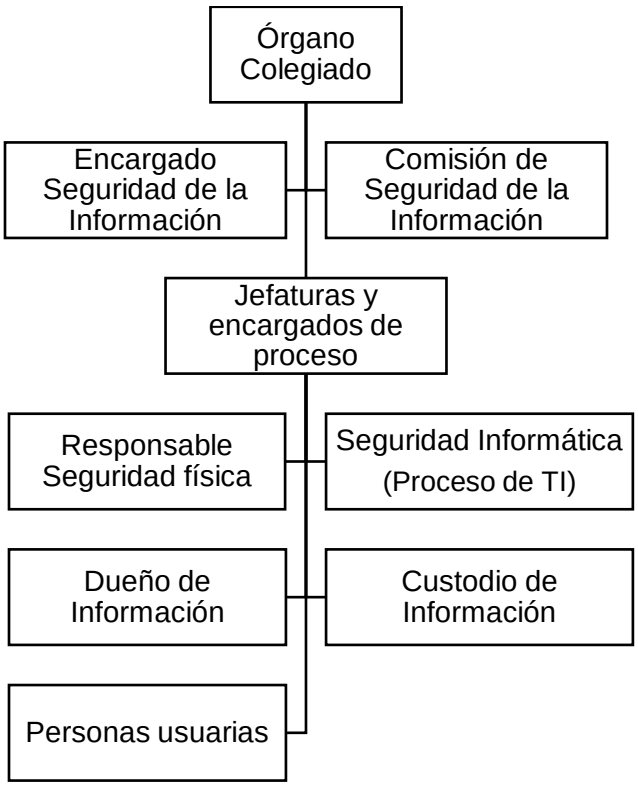

Ilustración 1: Estructura de la organización para la gestión de la seguridad de la información. Fuente Proceso de Tecnologías de la Información.

Artículo No. 3: De las responsabilidades del Máximo Jerarca (Órgano Colegiado).

Son responsabilidades del Máximo Jerarca:

a. Revisar y aprobar la política de seguridad de la información asegurando que sea adecuada para la Institución.
b. Evaluar y aprobar las iniciativas principales para mejorar la seguridad de la información en la Institución.
c. Direccionar a las dependencias correspondientes para que esta política sea difundida entre todo el personal la Política de Seguridad de la Información.
d. Asegurar que la Política de Seguridad de la Información sea de conocimiento y aplicación de todos los usuarios en la Institución y se comprometan al cumplimiento de la misma.
e. Supervisar el rendimiento de la gestión de seguridad de la información.

Artículo No. 4. De los roles y responsabilidad de la Comisión de Seguridad de la Información

a. **Finalidad de la Comisión de seguridad de la información:** Generar directrices para mejorar el proceso de gestión y protección de la seguridad de la información ya que es designado para la implementación y cumplimiento de la normativa relacionada con seguridad de la información en la Institución.

b. **Conformación:** estará conformado por los siguientes miembros:
   - Director/a Administrativo Financiero
   - Juez/a Tramitador/a
   - Encargado/a del Proceso de Tecnologías de Información

Los miembros nombrarán dentro de su seno un presidente y un secretario que podría ser miembro del mismo comité o externo a éste.

c. Responsabilidades de la Comisión de Seguridad de la Información:

- Revisar y proponer la Política de Seguridad de la Información verificando su efectividad y correcta implementación.
- Presentar para aprobación del Máximo Jerarca, las propuestas de inclusión de roles y responsabilidades de seguridad en los manuales de organización y funciones de la Institución.
- Revisar la Política de Seguridad verificando su efectividad y correcta implementación.
- En conjunto con la Comisión de Control Interno, revisar los resultados de la evaluación de riesgos, seleccionar los controles de tratamiento de riesgo e incluir los riesgos en la Matriz de Riesgos del TRA.
- Emitir directrices para el cumplimiento de las políticas y procedimientos de seguridad de la información, incluyendo planes y programas de trabajo, capacitación y concientización.
- Proponer convenios con especialistas en seguridad de la información para recibir asesoría continua.
- Revisar criterios de clasificación de la información y asegurar que se mantiene un inventario de activos de información actualizado.
- Revisar y proponer ante el Máximo Jerarca, normas y procedimientos del proceso de gestión de seguridad.
- Revisar y dar seguimiento a las incidencias mayores de la seguridad de la información e informar al Máximo Jerarca.

- En conjunto con la Comisión de Control Interno, debe supervisar la ejecución periódica de la evaluación de riesgos y aprobar los planes de tratamiento de riesgos.

- Proponer políticas para administrar el riesgo de la seguridad de información.

d. Cese y actualización de los integrantes de la Comisión de Seguridad de la Información

Como se establece en el apartado Conformación, la Comisión de Seguridad estará conformada por titulares; sin embargo, el presidente de la Comisión de Seguridad de la Información deberá coordinar con el resto de los integrantes, la designación de la persona que lo sustituirá. En el momento que algún miembro de la comisión, cese en el ejercicio de su actividad será el suplente quien asuma el cargo.

e. Convocatorias y sesiones de la Comisión de Seguridad e Información

Se establece dos tipos de sesiones, a saber: ordinarias (planificadas) o sesiones extraordinarias (cuando se requiera).

f. **Periodicidad:** La periodicidad de reunión la define la comisión y debe guardar registros para evidenciar su funcionamiento, siendo al menos tres reuniones anuales, sin menoscabo que pueden realizarse las extraordinarias que se ameriten.

Estas reuniones podrán ser presenciales o virtuales, utilizando la plataforma tecnológica existente en el Tribunal Registral Administrativo.

g. **Convocatorias:** Para mantener el orden se debe establecer quien o quienes realizarán las convocatorias. Por ejemplo: “Las realiza el presidente, el Encargado de Seguridad de la Información o el secretario de la comisión por encargo del presidente; y serán notificadas por correo electrónico con mínimo 7 días de antelación”. En este caso

podrán realizarse reuniones planificadas de manera mensual y/o talleres de trabajo cuando se requiera en equipo o únicamente con el especialista del equipo en materia de revisión. Se deben dejar registros de las reuniones y/o talleres de trabajo.

h. **Evidencia de los acuerdos:** La evidencia de las sesiones y de los acuerdos tomados por la Comisión de Seguridad de la Información se gestionará conforme se establece en el Manual de Comisiones del Tribunal Registral Administrativo. La comisión realizará seguimiento del cumplimiento de los acuerdos en cada sesión.

i. **Seguimiento de planes de trabajo:** La agenda de las reuniones podrá contemplar lo siguiente, dependiendo de las temáticas de los proyectos que se encuentren en desarrollo:

- Seguimiento de los programas y planes de trabajo de las distintas áreas o dependencias a las cuales se les haya asignado responsabilidad por la implementación de controles a nivel operativo.
- Plan de concientización en materia de seguridad de la información; seguimiento del plan de concientización.
- Revisión del proceso de seguridad (Inspecciones o auditorías internas); revisión de los resultados de las evaluaciones.
- Principales incidentes de seguridad ocurridos o detectadas (riesgos)
- Seguimiento a la gestión con equipos de trabajo de apoyo.
- Seguimiento al cumplimiento de acuerdos.
- Otros que considere pertinentes

Artículo No. 5. Del rol del dueño de la información

a. **Custodio de activos de información:** Se establecen como dueños de la información a los encargados de proceso, quienes son responsables de los activos de información que utilicen y generen en su gestión diaria, de tal forma que las decisiones que tomen inciden en la confidencialidad, integridad y disponibilidad de la información.

b. **Responsabilidades:** El rol del dueño de la información comprenderá lo siguiente:

- Identificar toda la información y procesamiento de ésta, correspondiente a su área de responsabilidad cualquiera sea su forma y medio de almacenamiento y gestión.
- Definir el grado de criticidad los datos de su propiedad (datos que produce y por ello el principal responsable por su gestión) de acuerdo con el grado de criticidad de éstos.
- Ante algún eventual cambio en la clasificación de la información, debe comunicar a la persona responsable del proceso de Archivo y encargada de Seguridad de la Información para que se realicen los cambios asegurando que se mantenga actualizada la documentación.
- Velar por la seguridad de sus datos, procurando la correcta aplicación de mecanismos orientados a la mitigación de riesgos.
- Participar activamente en la definición del valor de la información para la Institución, de manera que se puedan definir los controles apropiados para protegerla.
- Establecer y autorizar los criterios y niveles de acceso a la información.

Artículo No. 6. Del rol de las personas usuarias del TRA

a. **Custodio de activos de información:** Este rol corresponde con la persona funcionaria del TRA autorizada para acceder a los activos de información de acuerdo con su puesto o función.

b. **Responsabilidades:** Sus responsabilidades serán las siguientes:

- Conocer y cumplir con la Política General de Seguridad de la Información, normas, procedimientos, y demás definiciones de seguridad de la información implementadas, controles en materia de seguridad.
- Emplear los activos de información de la Institución solamente para los fines propios del mismo, solo para el cumplimiento de sus funciones y/o fines institucionales.
- Reportar los eventos o incidentes ocurridos sobre los activos de información, utilizando los canales dispuestos en la Institución para tal fin.
- Reportar posibles debilidades de seguridad de la información detectadas.
- Mantener la confidencialidad de las contraseñas utilizadas.
- Tomar las medidas necesarias e inmediatas para no exponer la información confidencial y uso interno a una lectura no autorizada por parte de un tercero.
- Participar activamente en las charlas, talleres y capacitaciones relativas a la seguridad de la información.

Artículo No. 7: Del rol y responsabilidades del Encargado de seguridad de la información.

a. Administrar y coordinar la ejecución del proceso de seguridad de la información.
b. Recomendar disposiciones de seguridad para que sean incorporadas por las áreas o dependencias que correspondan a nivel de estándares y procedimientos de seguridad de la información.
c. Coadyuvar en la implementación de los aspectos de seguridad en las plataformas tecnológicas que soportan los procesos de la Institución.
d. Coadyuvar en la emisión de directrices para que las dependencias que las dependencias documenten los procedimientos de seguridad de la información y Coadyuvar con la Comisión de Seguridad de la Información para desarrollar, mantener y comunicar las políticas, estándares y procedimientos para la gestión segura de la información.
e. Coadyuvar en la generación de procedimientos para dar respuesta a incidentes, para atender los problemas relacionados a la seguridad de la información dentro de la Institución.
f. Incorporar en el Plan de Capacitación definido por el Consejo Académico procesos de capacitación para generar cultura de seguridad de la información.
g. Asegurar que sea administrado, custodiado, monitoreado el buen estado de los equipos tecnológicos de apoyo a la seguridad física y ambiental.

h. Proponer políticas orientadas a mejorar el control de acceso en la seguridad física.
i. Reportar cualquier asunto relacionado a la materia a la Comisión de Seguridad de la Información.

Artículo No. 8. Del rol de la Seguridad Informática realizada por la Dependencia encargada del Proceso de Tecnologías de Información.

a. Diseñar y proponer al Órgano Colegiado estrategias de seguridad informática.
b. Proponer medidas de seguridad para la gestión de toda la información existente (bases de datos, base de correos, planillas electrónicas, documentos electrónicos, firewall, dispositivos de filtrado IPS/IDS).
c. Administrar y brindar soporte sobre las medidas y herramientas de seguridad implementadas en la organización, entre los cuales se encuentran: gestionar y monitorear los accesos a los recursos, administrar llaves criptográficas, monitorear las actualizaciones de seguridad, administrar el acceso lógico a los recursos tecnológicos como aplicativos, base de datos, carpetas compartidas, y cualquier otro recurso en formato electrónico.
d. Gestionar los riesgos e incidentes de seguridad utilizando el procedimiento establecido en la Institución.
e. Analizar e implementar, como parte del proceso de mejora continua, nuevas medidas y herramientas de seguridad informática.

Artículo No. 9: Del rol y responsabilidades del Custodio de los activos de la información

a. **Custodio de activos de información:** Es la persona, equipo o área, que mantiene bajo su responsabilidad la protección de los datos, en función a la clasificación de la información realizada por su dueño; se encarga de administrar, almacenar y aplica las medias de seguridad que se definan de acuerdo con el valor de los activos de información, definido por el dueño de la información. Las dependencias que custodien activos de valor, documentación en formatos físicos e información en medios electrónicos asumirán este rol. La dependencia encargada de Archivo y la dependencia encargada del Proceso de Gestión de TI son custodios, asimismo todo funcionario al cual se le han asignado activos físicos e información a la cual se le ha conferido el acceso.

b. Las responsabilidades del Custodio de los activos de la información:

- Cumplir con los requerimientos de protección de la información establecidos en la Institución y los especificados por el propietario o dueño de la información.

- Apoyar en la gestión de los riesgos de seguridad de la información.
- Coadyuvar en la implementación, operación y mantenimiento de los controles de seguridad de la información aplicados a los activos de información que se encuentran bajo su custodia.
- Tomar las medidas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los activos de información que se encuentran bajo su custodia y que son entregados a las personas usuarias.
- En el caso de la dependencia encargada del proceso de Gestión de TI:
    a. Administrar los accesos y asignarlos a las personas usuarias de los activos de información de acuerdo con las especificaciones establecidas por los propietarios o dueños.
    b. Coordinar y ejecutar los procedimientos de respaldo, recuperación y restauración de la información.

Artículo No. 10. Del rol y responsabilidades del responsable de la Seguridad Física

a. **Responsable de la Seguridad Física:** Persona o dependencia encargada de coordinar e implementar la seguridad física institucional; y es responsable de la aplicación de los controles de seguridad física de los principales activos de información.

b. Responsabilidades del responsable de la Seguridad Física:

- Identificar, evaluar y proponer planes de tratamiento sobre los riesgos físicos.
- Informar a la jefatura inmediata y a las personas Encargada de Seguridad de la Información sobre los riesgos de seguridad física y el estado de los controles a implementarse.
- Asegurar que las medidas específicas de seguridad física se integren adecuadamente dentro del marco de seguridad de la información.
- Proponer y mantener los planes de seguridad física, y en conjunto con la Comisión de Atención de Emergencias mantener los planes y procedimientos de evacuación acorde con las políticas de Seguridad de la Información.
- Mantener vigentes los controles de seguridad física.
- Solicitar y asegurar la inclusión de entrenamiento y capacitación con relación a la Seguridad Física para todas las personas colaboradores de la Institución, dentro del Plan de Capacitación y Concientización elaborado por la dependencia encargada del Proceso de Gestión de Recurso Humano.
- Evaluar y recomendar especificaciones técnicas para la seguridad de la información, entro de su ámbito de trabajo.

CAPÍTULO III:
SEGURIDAD DE LOS RECURSOS HUMANOS

Artículo No. 11: Del proceso de reclutamiento y selección de los servidores del Tribunal Registral Administrativo

El proceso de Recursos Humanos debe realizar las siguientes actividades relacionadas con el reclutamiento y selección del personal administrativo para el TRA y que son fundamentales para la seguridad de la información:

a. Realizar todas las verificaciones necesarias para confirmar la veracidad de la información suministrada por el candidato a ocupar un cargo antes de su vinculación definitiva.
b. Informar al personal dentro del proceso de integración mediante la inducción la existencia de políticas contenidas en el presente manual.
c. Ninguna persona usuaria, ya sea funcionaria o tercero recibirá credenciales de acceso a la plataforma tecnológica, los servicios de red y los sistemas de información o aplicaciones, hasta que no acepte formalmente la Política de Seguridad de la Información vigente.

Artículo No. 12: Durante el empleo (Proceso de integración del personal)

El Máximo Jerarca, representado por la figura del Órgano Colegiado, con el fin de proteger la información y los recursos de procesamiento del TRA, y como demostración de apoyo a la implementación del Proceso de Gestión de Seguridad de la Información, promoverá la cultura de seguridad de la información entre el personal del TRA, tendrá las siguientes actividades:

a. Aprobar la implementación de políticas de seguridad de la información.
b. Promover la importancia de la seguridad de la información entre todo el personal, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares establecidos.
c. En todos aquellos casos de incumplimiento al presente manual de políticas de seguridad de la información y de conformidad con procedimiento y las respectivas sanciones que están establecidas por principio de legalidad en las respectivas leyes y reglamentos, el Máximo Jerarca debe decirse aplicar las medidas sancionatorias de acuerdo con lo establecido en el Reglamento Autónomo de Servicio.

d. El Director Administrativo comunicará por los medios correspondientes la emisión de normativa vinculada al proceso de gestión de seguridad de la información.

El Consejo Académico:

a. Los eventos de capacitación y sensibilización en seguridad de la información serán coordinados con el Consejo Académico por la dependencia encargada del Proceso de Tecnologías de Información, e integrados a un programa de sensibilización en seguridad de la información que se realizará de manera anual y para el cual deberán proveerse los recursos para su ejecución y controlar la asistencia. La dependencia encargada del Proceso de Gestión del Recurso Humano deberá llevar registro (en expediente de personal) de la asistencia a actividades de capacitación en seguridad de la información.

Todo el personal que por su cargo hagan uso o participe de la cadena de custodia para la preservación y conservación de la información y activos a los que el TRA le ha conferido el acceso, debe:

b. Cumplir a todo lo indicado en el presente manual de políticas de seguridad de la información según les corresponda (todos aquellos apartados y responsabilidades de este documento que hagan referencia a todo el personal).
c. Asistir a las charlas y eventos a los cuales sean convocados como parte del programa de sensibilización en seguridad de la información. En aquellos casos de fuerza mayor y donde la persona no haya asistido al evento, deberá proporcionársele el acceso o material usado durante éste.
d. Todo el personal debe ser cuidadoso de no divulgar información confidencial del TRA ni por escrito ni en forma verbal. Igualmente, esto aplica para situaciones donde la revelación de información pueda causar un impacto operativo, reputacional o legal para el TRA.

Artículo No. 13: Terminación de la relación laboral y cambio de empleo

El TRA asegurará que, en caso de desvinculación con la institución, cambios en puestos o nuevos nombramientos, la ejecución de nuevas labores se realice de forma ordenada, controlada y segura, por lo tanto, define lo siguiente:

a. La dependencia encargada del Proceso de Gestión del Recurso Humano informará a la persona encargada del Proceso de Tecnologías de Información, sobre la finalización de funciones por parte de una persona funcionaria, nuevos nombramientos o bien, cuando una persona colaboradora cambie de puesto, a efecto de que se tomen las previsiones respectivas.

CAPÍTULO IV:
GESTIÓN DE ACTIVOS

Artículo No. 14: Política de responsabilidad por los activos de información

La información, los sistemas, los servicios y los equipos (estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, servidores, aplicaciones, teléfonos, entre otros) del TRA, son activos de la Institución y se proporcionan a los funcionarios y a terceros autorizados, para cumplir con los propósitos institucionales.

Todos los activos de información del TRA, deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que establezca la Administración debido a la sensibilidad de la información y la normativa aplicable.

a. Responsabilidad por los activos de la información

- Cada jefatura y encargado de proceso, debe actuar como responsable de la información física y electrónica de la dependencia a cargo, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Cada jefatura y encargado de proceso como responsable de los activos de información debe generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones que establezca la Administración para la clasificación de la información con el apoyo del encargado del Proceso de Tecnologías de Información y dependencia encargada del Proceso de Archivo quien establecerá un Cuadro de Clasificación de la Información utilizando como insumo tablas de plazos y las necesidades de cada dueño de proceso.
- Cada jefatura y encargado de proceso como responsable de los activos de información al menos una vez cada 6 meses, debe monitorear la validez de los usuarios y sus perfiles de acceso a la información.

- En aquellos casos en los cuales se tengan indicios de la vinculación de una persona usuaria con incidente de seguridad, la dependencia encargada del Proceso de Tecnologías de Información puede realizar monitoreo sobre los activos de información asignados a ésta. Este procedimiento debe realizarse bajo a autorización de la persona usuaria involucrada.
- Los activos de información del TRA deben ser utilizados por todo el personal de acuerdo con las políticas contenidas en el presente manual y según la normatividad vigente nacional. Esto con el fin de evitar un impacto operativo, legal o reputacional para el TRA.
- En casos excepcionales, si algún miembro necesita utilizar equipos propios diferentes a los proporcionados por la Institución, deben solicitar la autorización, verificación y registro de la dependencia encargada del Proceso de Tecnologías de Información.
- Todas las personas funcionarias y terceras partes deben cumplir con los controles mínimos de seguridad establecidos (antivirus, sistema operativo con ciertos parches de seguridad), por la dependencia encargada del Proceso de Tecnologías de Información, para poder conectarse a la red de la Institución.
- Las personas funcionarias en el momento de desvinculación o finalización de labores con el TRA deben realizar la entrega de su puesto de trabajo a su jefatura inmediata, a la vez que también deben entregar de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo de la Institución para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

b. Nomenclatura para asignar nombre de equipo de cómputo

- El objetivo es establecer el estándar para la nomenclatura de todos los equipos de cómputo del Tribunal Registral Administrativo.
- El nombre de los equipos de cómputo deberá tener un máximo de quince (15) caracteres.
- El nombre de los equipos de cómputo deberá tener el siguiente formato:
  [Acrónico institucional] [Tipo de equipo] [Número Consecutivo][Número de Patrimonio]
- Acrónimo institucional: Se refiere a que se debe de utilizar **TRA**
- Tipo de equipo: A continuación, se lista los tipos de equipo.

Código	Tipo de equipo
PC	Computadora de escritorio
LT	Portátil
SR	Servidor físico
IM	Impresora

- Número consecutivo: Deberá seguir el orden de la numeración que gestiona el encargado de Tecnologías de Información.
- Número de patrimonio: Se utilizará los últimos cuatro dígitos de la numeración del patrimonio asignada por el encargado de bienes de la institución.

- Se lista un ejemplo:

- **TRA-LT-001-1018**

- Para el nombre de los servidores virtuales o máquinas virtuales se hará una excepción a la nomenclatura debido a que no poseen número de patrimonio. Por lo anterior se definirá de la siguiente manera:
- El nombre de los equipos de cómputo deberá tener el siguiente formato:
  [Acrónico institucional] [Tipo de equipo] [Número Consecutivo]
- Acrónimo institucional: Se refiere a que se debe de utilizar **TRA**
- Tipo de equipo: A continuación, se lista los tipos de equipo.

Código	Tipo de equipo
SRV	Servidor Virtual

- Número consecutivo: Deberá seguir el orden de la numeración que gestiona el encargado de Tecnologías de Información.

- Se lista un ejemplo:
  - **TRA-SRV-001**
- El nombre de los equipos tanto físicos como virtuales, deberá ser único dentro del dominio de la red de la institución.
- La aplicación de este artículo deberá estar a cargo del proceso de Tecnologías de Información.

Artículo No. 14.1: Clasificación de la información

El TRA definirá los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad y el encargado de Seguridad de la Información en conjunto con la dependencia encargada del Proceso de Archivo y la dependencia del Proceso de Gestión de Tecnologías, generará un Cuadro de Clasificación de la Información para que los propietarios de ésta la cataloguen y determinen los controles requeridos para su protección.

Toda la información debe ser identificada, clasificada y documentada de acuerdo con la Cuadro de Clasificación de la Información que deberá ser establecida por la dependencia encargada de Archivo utilizando como insumo tablas de plazos y las necesidades de cada dueño de proceso.

El Cuadro de Clasificación de la Información permitirá categorizar aquella información a la que se le deben los controles técnicos y administrativos con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos en función de su nivel de clasificación.

a. Normas para la clasificación y manejo de la información

- El personal del TRA deben cumplir con los lineamientos establecidos en el Cuadro de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Institución.
- La dependencia encargada del Proceso de Archivo debe tener un período de almacenamiento para la información física y digital, el cual puede ser dictaminado por requerimientos legales o sustantivos de la Institución; este período debe ser indicado previamente por el propietario de la información y cuando se cumpla el período de expiración, toda la información debe ser eliminada adecuadamente. La dependencia debe considerar los periodos de retención de documentos según lo

establece según lo que establezca la ley y la Comisión Nacional de Selección y Eliminación de Documentos (CNSED).

- Todo el personal debe tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes:
    a. Verificar las áreas vecinas a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales.
    b. Recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Para cumplir con la clasificación a continuación se presentan los tipos de prioridad para la información:
    a. Pública: estará la información que se puede compartir
    b. Uso interno: estará la información de interés para la Institución, en general.
    c. Información confidencial: estará la información de interés solo para un área en particular o por disposición de la ley (datos sensibles, privados, datos personales de acceso restringido según Ley de Protección de la Persona frente al tratamiento de sus Datos Personales).
- Toda jefatura o encargado de proceso debe realizar la entrega de toda la información a quien lo suceda en el cargo.
- Toda jefatura o encargado de proceso debe resguardar la información en formato electrónico, de carácter histórico, está quedará documentada como activo del área.
- Ningún miembro del personal o tercero deberá poseer material o información confidencial de la Institución, para usos no propios de su responsabilidad.

b. Etiquetado de la información

- Toda información que se almacene en algún soporte físico incluyendo papel o en medios magnéticos u ópticos (CD/DVD) se deberá etiquetar usando los mismos niveles establecidos en clasificación de la información.
- Las jefaturas o encargados de proceso son responsables de la información contenida en las unidades a su cargo deben delimitar las responsabilidades de sus subordinados y determinar quién está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

Artículo No. 15: Manejo de los soportes de almacenamiento

El TRA evitará la divulgación no autorizada, la modificación, eliminación o destrucción de la información almacenada en los medios de almacenamiento dispuestos para tal fin.

a. Gestión de soporte extraíbles

- La dependencia encargada del Proceso de Tecnologías de Información, como responsable de proporcionar los medios, mecanismos o herramientas tecnológicas realizará la gestión de medios extraíbles de acuerdo con las necesidades de cada usuario respecto a las labores desempeñadas.
- Los equipos de cómputo tienen autorizado el manejo de USB y unidades reproductoras de CD/DVD; por lo tanto, deben cumplir con los siguientes requisitos:
    a. Tener habilitado el escaneo automático de virus.
    b. Tener configurado en el software de antivirus el bloqueo de la reproducción automáticas de archivos ejecutables.

2. Eliminación de soportes

- La dependencia encargada del Proceso de Tecnologías de Información debe velar porque la información será eliminada de los medios de almacenamiento de forma segura cuando ya no sea necesaria, utilizando procedimientos y herramientas de borrado seguro, garantizando que no queden rastros de ésta.

3. Soportes físicos e información en tránsito

- La dependencia encargada del Proceso de Tecnologías de Información debe garantizar que los medios que contienen información confidencial estén protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte.
- La dependencia encargada del Proceso de Tecnologías de Información debe garantizar que la información que transita a través de la red cuenta con los protocolos de seguridad necesarios, asegurado su confidencialidad, disponibilidad e integridad. Para este efecto debe establecer un procedimiento de gestión segura de la transferencia de información que atienda a las solicitudes de información por terceras partes.
- La dependencia encargada del Proceso de Tecnologías de Información debe implementar la utilización de protocolos de seguridad para el cifrado de las claves.

CAPÍTULO V:
CONTROL DE ACCESO

Artículo No. 16: Política de control de acceso

El TRA garantizará entornos con controles de acceso idóneos, los cuales aseguren el perímetro, tanto en oficinas, centro de datos y cualquier otro recinto donde se almacene y gestione información sensible, así como en entornos abiertos para evitar el acceso no autorizado a ellos.

Asimismo, controlará las amenazas físicas externas y velará por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información digitales y físicos.

a. La dependencia encargada del Proceso de Tecnologías de Información en conjunto con la dependencia encargada de Mantenimiento, deben asegurar la implantación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con los que se debe contar para la protección del centro de procesamiento de datos y cuartos de comunicaciones.
b. Las dependencias responsables de las áreas como el centro de datos, el archivo institucional o cualquier otra área en donde procesa o almacena información sensible y que son consideradas seguras, tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:
    - Las áreas que se catalogan como seguras deben permanecer cerradas y custodiadas.
    - El acceso a áreas seguras donde debe ser limitado únicamente a personas autorizadas.

c. Acceso a redes y a servicios en red

- La dependencia encargada del Proceso de Tecnologías de Información como responsable de las redes de datos y los recursos de red de la Institución, debe velar porque dichas redes sean debidamente protegidas contra accesos no autorizados por medio de mecanismos de control de acceso lógico.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Institución

- La dependencia encargada del Proceso de Tecnologías de Información debe asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer controles para la identificación y autenticación (ejemplo, integración con directorio activo, redes VPN) de los usuarios provistos por terceras partes a las redes o recursos de red del TRA, así como velar por la aceptación de las responsabilidades de dichos terceros en cuanto a las Políticas de Seguridad de la Información.
- La dependencia encargada del Proceso de Tecnologías de Información debe suministrar una herramienta para realizar conexiones remotas a la red de área local del TRA de manera segura para todo el personal y su labor así lo requiera, la cual debe ser aprobada, registrada y auditada.
- La dependencia encargada del Proceso de Tecnologías de Información debe contar con un procedimiento de creación de cuentas, donde estén definidas las condiciones de autorización y acuerdos de confidencialidad respectivos.
- Todo el personal debe firmar a manera de acuse de recibo y aceptación de un documento formal, otorgado por la dependencia encargada del Proceso de Tecnologías de Información con el detalle de los accesos lógico a los sistemas de información de la Institución, según sea el caso.
- Toda persona funcionaria y terceros que deseen que los equipos de cómputo personales accedan a la red de datos de la Institución deben cumplir con todos los requisitos o controles para autenticarse en ésta y únicamente podrán realizar las tareas para las que fueron autorizados.
- Toda persona funcionaria y terceros deben contar con una autorización y con los mecanismos permitidos por la dependencia encargada del Proceso de Tecnologías de Información, para realizar una conexión remota por medio de virtual privada a equipos conectados a la red interna desde fuera de la misma.

Artículo No. 17: Gestión de acceso de personas usuarias

a. Política de administración de acceso de personas usuarias

- El TRA, a través de TI establecerá privilegios para el control de acceso lógico de cada usuario o grupo de personas usuarias a las redes de datos, los recursos tecnológicos y los sistemas de información de la Institución. Asimismo, velará porque todo el personal y proveedores tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

- El Encargado del Proceso de Tecnologías de Información definirá un procedimiento formal para la administración del acceso de los usuarios a las redes de datos, los recursos tecnológicos y sistemas de información de la Institución; que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
- Cuando sea necesario, las jefaturas o encargados de procesos deben gestionar la creación, modificación, bloqueo o eliminación de las personas s usuarias y permisos a los diferentes sistemas de información y recursos tecnológicos ante dependencia encargada del Proceso de Tecnologías de Información quien será el encargado de ejecutar las labores a nivel tecnológico y de sistemas de información.
- La dependencia encargada del Proceso de Tecnologías de Información debe definir los lineamientos para las características que deben contener las contraseñas que se aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna.
- La dependencia encargada del Proceso de Tecnologías de Información debe deshabilitar o eliminar los usuarios o perfiles de usuario predeterminados que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica.
- La dependencia encargada del Proceso de Tecnologías de Información en conjunto con los propietarios de los activos de información debe autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la Institución, según sea el caso.
- Los propietarios de los activos de información (jefaturas o dependencias encargadas de procesos) deben verificar y ratificar periódicamente (cada seis meses) todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

b. Política de responsabilidades de acceso de las personas usuarias

- Las personas usuarias, de los recursos tecnológicos y los sistemas de información, realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.
- Todo el personal y terceros que hacen uso de la plataforma tecnológica, los servicios de red y los sistemas de información del TRA, deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Ninguna persona debe compartir sus cuentas de usuario y contraseñas asignados para el ingreso a los servicios de red y los sistemas de información con otros miembros de la Institución o terceros.

- Todo el personal y terceros que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información que la Institución ofrece deben acogerse a las normas establecidas para la configuración de contraseñas designadas por ésta.

c. Registro y cancelación del registro de personas usuarias

- La dependencia encargada del Proceso de Tecnologías de Información debe registrar todos los usuarios en la Base de Datos o Matriz de Usuarios y Roles.
- La creación de un nuevo usuario o solicitud para la asignación de otros roles dentro de cualquier sistema de información deberá acompañarse por la solicitud debidamente firmado por su jefatura o encargado, de lo contrario no se le dará trámite a la requisición.

Artículo No. 18: Control de acceso a sistemas y aplicaciones

a. Restricción de acceso a información

- Todo el personal y terceros serán responsables por las credenciales (usuario y contraseña) que le sean asignadas y que reciben para el uso y acceso de los recursos.
- Todo el personal, visitantes y terceros, deberán autenticarse en los mecanismos de control de acceso provistos por la dependencia encargada del Proceso de Tecnologías de Información antes de poder usar la infraestructura tecnológica del TRA.
- El personal no debe proporcionar información de los mecanismos de control de acceso en las instalaciones e infraestructura tecnológica del TRA a personal externo, a menos que se tenga el visto bueno del dueño de la información y de su jefe inmediato.
- El personal que acceda a la infraestructura tecnológica del TRA, debe contar con un identificador de usuario (ID) único y personalizado.

b. Procedimiento de inicio de sesión segura

- La dependencia encargada del Proceso de Tecnologías de Información debe implementar los controles necesarios (ejemplo, contraseñas fuertes, bloqueo de inicio de sesión después de intentos fallidos) para proteger los servicios de información de intentos de inicio de sesión mediante ataques de fuerza bruta.

- La dependencia encargada del Proceso de Tecnologías de Información debe generar mensajes de advertencia general indicando que solo los usuarios autorizados pueden acceder al equipo de cómputo.
- La dependencia encargada del Proceso de Tecnologías de Información debe validar la información de ingreso solamente al completar todos los datos de entrada. Si presenta una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.
- La dependencia encargada del Proceso de Tecnologías de Información debe habilitar el registro de los intentos exitosos y fallidos de acuerdo con los perfiles de los usuarios en los sistemas de información necesarios.
- La dependencia encargada del Proceso de Tecnologías de Información debe garantizar la transmisión segura de contraseñas sobre la red.
- La dependencia encargada del Proceso de Tecnologías de Información debe asegurar la terminación de sesiones inactivas después de un período de inactividad de cinco minutos, teniendo especial cuidado con lugares de alto riesgo, tales como áreas públicas o externas por fuera de la organización o en dispositivos móviles.

CAPÍTULO VI:
CIFRADO

Artículo No. 19: Controles criptográficos

El TRA asegurará el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información confidencial de la Institución al momento de almacenarse o transmitirse.

a. Política de uso de los controles criptográficos

- La dependencia encargada del Proceso de Tecnologías de Información debe proporcionar los mecanismos o herramientas necesarias para asegurar la protección de claves de acceso a la red de datos, los sistemas de información, datos y servicios de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información debe proporcionar los mecanismos de cifrado necesarios para asegurar que la transmisión de información confidencial de forma interna o externa se realice de forma segura.
- La dependencia encargada del Proceso de Tecnologías de Información debe proporcionar los mecanismos o herramientas necesarias para cifrar la información confidencial de la Institución, resguardada por los propietarios de la información (jefaturas o dependencia encargada de proceso).

CAPÍTULO VII:
SEGURIDAD FÍSICA Y AMBIENTAL

Artículo No. 20: Áreas seguras

El TRA asegurará la implementación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones, minimicen la ocurrencia de riesgos producto de amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. Áreas donde se almacene información en soporte físico también debe ser considerada como una zona segura.

a. Controles físicos de entrada

- Cualquier persona (funcionario o tercero), que tenga acceso a las instalaciones del TRA, deberá registrar los equipos de cómputo que no sean de propiedad de la Institución, en bitácora custodiada por el personal de seguridad en la recepción del edificio y de acuerdo con los procedimientos definidos por la dependencia encargada del Proceso de Tecnologías de Información.
- Toda aquella persona funcionaria y terceros, que requieran ingresar al centro de datos y a los centros de cableado, deben realizar las solicitudes de acceso a dependencia encargada del Proceso de Tecnologías de Información. Adicional, los responsables deben realizar un registro del ingreso de los visitantes en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Las personas funcionarias y terceros que deseen ingresar a los centros de cómputo y a los centros de cableado deben realizar el ingreso acompañados de un funcionario de la dependencia responsable de los mismos.
- Todo el personal y terceros deben cumplir completamente con los controles físicos implementados por la Institución, ya que los ingresos y salidas a las instalaciones del TRA deben ser registrados.
- Todo el personal y terceros deben portar gafete que los identifica como tales en un lugar visible, mientras se encuentren en las instalaciones de la Institución; en caso de pérdida deben reportarlo a la mayor brevedad posible.

- Todo el personal y terceros no deben intentar ingresar a áreas a las cuales no tengan autorización.
- La dependencia encargada del Proceso de Tecnologías de Información y que tiene bajo su custodia el centro de datos y cuartos de cableado deben modificar de manera inmediata los privilegios de acceso físico a estos sitios, en situaciones de desvinculación o cambio en las labores de una persona autorizada.
- La dependencia encargada del Proceso de Tecnologías de Información debe velar por las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en estos sitios. Para cumplir con esto deben existir:
    a. Sistemas de control ambiental de temperatura y humedad.
    b. Sistemas de extinción de incendios.
    c. Sistemas de vigilancia y monitoreo
    d. Alarmas en caso de detectarse condiciones ambientales inapropiadas.
- La dependencia encargada del Proceso de Tecnologías de Información que tiene bajo su custodia el centro de cómputo y centros de cableado, en conjunto con la dependencia encargada del Proceso de Mantenimiento, deben velar porque los recursos de la plataforma tecnológica, ubicados en estos sitios, se encuentren protegidos contra fallas o interrupciones eléctricas.
- La dependencia encargada del Proceso de Tecnologías de Información que tiene bajo su custodia el centro de cómputo y centros de cableado, en conjunto con la dependencia encargada del Proceso de Mantenimiento, deben certificar que estos sitios se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La dependencia encargada del Proceso de Tecnologías de Información que tiene bajo su custodia el centro de cómputo y centros de cableado, en conjunto con la dependencia encargada del Proceso de Mantenimiento, deben asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y previamente autorizado e identificado.
- La dependencia encargada del Proceso de Tecnologías de Información que tiene bajo su custodia centros de cómputo y centros de cableado deben llevar control de la programación de los mantenimientos preventivos a estos sitios, teniendo en cuenta los niveles de servicio acordados con los responsables de los servicios particulares y acorde a la operación de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información que tiene bajo su custodia el centro de cómputo y centros de cableado, en conjunto con la dependencia encargada del Proceso de Mantenimiento, deben velar porque los niveles de temperatura y humedad relativa en estos sitios estén dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado según sea el caso.

- La dependencia encargada del Proceso de Mantenimiento debe solicitar mantenimientos preventivos y pruebas de funcionalidad del sistema de sistemas de alimentación ininterrumpida (UPS) y plantas eléctricas, de los sistemas de detección de incendios y del sistema de aire acondicionado.

b. Protección sobre amenazas externas o ambientales

- La dependencia encargada del Proceso de Tecnologías de Información que tiene bajo su custodia el centro de cómputo y centros de cableado, en conjunto con la dependencia encargada del Proceso de Mantenimiento, deben monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos.
- El TRA debe designar y aplicar protección física para desastres como: fuego, inundación, terremoto, explosión, disturbio civil y otras formas de desastre natural o humano.
- La dependencia encargada del Proceso de Tecnologías de Información que tiene bajo su custodia el centro de cómputo y centros de cableado, en conjunto con la dependencia encargada del Proceso de Mantenimiento, deben velar por el ambiente adecuado para los activos informáticos como ventilación, iluminación, regulación de corriente, entre otros.

c. Trabajo en áreas seguras

El TRA debe mantener áreas seguras para la gestión, almacenamiento y procesamiento de información en la Institución (centro de datos, el archivo institucional o cualquier otra área en donde procesa o almacena información sensible). Las áreas deben contar con:

- Protecciones físicas y ambientales, acordes con el valor y la necesidad de aseguramiento de los activos que se protegen.
- Definición de perímetros de seguridad.
- Controles de acceso físicos.
- Seguridad para protección de los equipos.
- Seguridad en el suministro eléctrico y cableado.
- Condiciones ambientales adecuadas de operación.
- Sistemas de contención, detección y extinción de incendios.

Artículo No. 21: De la protección de los Equipos

a. Protección sobre amenazas externas o ambientales

- Las personas funcionarias y terceros no deben mover o reubicar los equipos de cómputo pertenecientes al TRA, instalar o desinstalar dispositivos, ni retirar marcas, logotipos ni hologramas de estos sin la autorización de la dependencia encargada del Proceso de Tecnologías de Información.
- De conformidad con el Manual de Contratación Administrativa y Bienes, la dependencia encargada del Proceso de Proveeduría Institucional debe resguardar los activos de información de soporte (equipos tecnológicos) y mantendrá un control de asignación de bienes por cada funcionario.
- Todo el personal debe conservar los equipos de cómputo en la ubicación autorizada por la dependencia encargada del Proceso de Tecnologías de Información.
- Todo el personal debe utilizar el equipo de cómputo asignado para uso exclusivo de las funciones del cargo que desempeñan en TRA.
- El personal debe solicitar la capacitación necesaria para el correcto manejo de las herramientas informáticas que requieren para realizar sus labores, a fin de evitar riesgos por mal uso y para aprovechar al máximo los recursos proporcionados por la Institución.
- El personal y terceros no deben consumir alimentos o ingerir líquidos mientras utilizan los equipos de cómputo en áreas sensibles de procesamiento de datos y gestión de información crítica.
- El personal debe informar a la dependencia encargada del Proceso de Tecnologías de Información cuando se requiera realizar cambios múltiples de los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, el plazo de anticipación de la solicitud dependerá de las implicaciones y cambios que se deban realizar.
- El personal y terceros no deben abrir o destapar los equipos de cómputo del TRA. Solo el personal de la dependencia encargada del Proceso de Tecnologías de Información está autorizado para realizar esta labor.

b. Seguridad del cableado

- La dependencia encargada del Proceso de Tecnologías de Información debe mantener los cables de red de los centros de datos claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- La dependencia encargada del Proceso de Tecnologías de Información y la dependencia encargada del Proceso de Mantenimiento, deben contar con los planos que describan las conexiones del cableado.

- La dependencia encargada del Proceso de Tecnologías de Información debe mantener el acceso a los centros de cableado solo para el personal autorizado.

c. Mantenimiento de equipos

- La dependencia encargada del Proceso de Tecnologías de Información es la responsable de llevar a cabo los servicios de mantenimiento y reparaciones al equipo informático, por medio de personal idóneo para la labor.
- El personal debe respaldar con copias de seguridad toda la información personal o confidencial que se encuentre en el equipo de cómputo asignado, previniendo así la pérdida involuntaria de la misma, derivada del proceso de reparación.
- La dependencia encargada del Proceso de Tecnologías de Información debe realizar procedimientos de borrado seguro en los equipos que se dan de baja y los equipos que son asignados a usuarios diferentes por temas de rotación.
- Todos los equipos asignados a todos los funcionarios del TRA deberán ser objeto de mantenimiento preventivo cada **tres(3) meses** por el personal de TI asignado. Sera responsabilidad de cada funcionario la obligación de firmar por parte del funcionario del Tribunal, el formulario "Inventario de equipo-revisión de programas de cómputo mantenimiento de hardware y software". En los casos de ausencia del funcionario, la persona encargada de firmar el formulario será el jefe inmediato o responsable del área.

d. Equipos de usuario desatendidos

- Toda persona debe bloquear la sesión de sus equipos de cómputo cuando no se encuentren en su lugar de trabajo. Esto con el fin que la sesión del usuario no quede activa con los privilegios que alguna otra persona pueda usar.
- Se debe instruir a los proveedores y terceras partes para bloquear la sesión de sus equipos desatendidos mientras se encuentren en las instalaciones del TRA.

e. Política de pantalla y escritorio limpios

- Todo el personal debe conservar el escritorio del equipo libre de información de uso interno o sensible (conforme la clasificación de datos y activos) propia de la Institución, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- La dependencia encargada del Proceso de Tecnologías de Información debe garantizar que los usuarios tengan la pantalla del equipo limpia o libre de archivos por medio de mecanismos adecuados para este fin.
- La dependencia encargada del Proceso de Tecnologías de Información debe aplicar un protector estándar en todas las estaciones de trabajo y equipos portátiles del TRA, de forma que se active luego de diez minutos sin uso.
- Todo el personal debe guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial o de uso interno.
- El personal no debe dejar desatendido el escritorio físico con documentos que pudiesen contener información sensible.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer las medidas de control necesarias que permitan comprobar el correcto cumplimiento de los puntos anteriores. Esto incluye el mantenimiento preventivo y correctivo que debe hacer trimestralmente revisando archivos existentes en los equipos con el objetivo de eliminar aquellos programas que no sean institucionales.

CAPÍTULO VIII:
SEGURIDAD DE LAS OPERACIONES

Artículo No. 22: Procedimientos operacionales y responsabilidades

- La dependencia encargada del Proceso de Tecnologías de Información debe realizar la documentación y actualización de los procedimientos relacionados con la operación y administración de los servicios de tecnologías de información de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información debe proporcionar a las personas funcionarias manuales de configuración y operación de los servicios de red, bases de datos y sistemas de información que conforman las diferentes plataformas.
- La dependencia encargada del Proceso de Tecnologías de Información debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de pruebas y producción, teniendo en cuenta consideraciones como:
    a. Controles para el intercambio de información entre los ambientes de desarrollo y producción.
    b. La inexistencia de compiladores, editores o fuentes en los ambientes de producción.
    c. Acceso diferente para cada uno de los ambientes.

a. Gestión de Cambios

- La dependencia encargada del Proceso de Tecnologías de Información establecerá los mecanismos para las solicitudes de cambios. De igual manera, coordinará y controlará los cambios realizados en los activos de información tecnológicos y los recursos informáticos.
- La dependencia encargada del Proceso de Tecnologías de Información garantizar que todo cambio realizado a un componente de la plataforma tecnológica, los cuales conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes no afecta la correcta operación de esta ni de otros servicios.
- La dependencia encargada del Proceso de Tecnologías de Información debe garantizar que todo cambio realizado sobre la plataforma tecnológica del TRA, quedará formalmente documentado desde su solicitud hasta su implementación.
- Los responsables de los activos de información tecnológicos y recursos informáticos (jefaturas o dependencia dueña de procesos) deben solicitar formalmente los

requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información utilizado para ello el procedimiento y herramientas que disponga la dependencia encargada del Proceso de Tecnologías de Información.

- La dependencia encargada del Proceso de Tecnologías de Información como custodios de los activos de información tecnológicos y recursos informáticos, deben garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios.

b. Gestión de capacidades

- La dependencia encargada del Proceso de Tecnologías de Información debe supervisar continuamente el uso de los recursos con el fin de realizar los pertinentes ajustes, revisar las proyecciones para las futuras necesidades de capacidad y asegurar el rendimiento del sistema requerido.
- La dependencia encargada del Proceso de Tecnologías de Información debe realizar estudios sobre las proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Aspectos por considerar:
    a. Consumo de recursos de procesadores, memorias, discos.
    b. Almacenamiento común.
    c. Servicios de impresión.
    d. Ancho de banda, internet y tráfico de las redes de datos.
    e. Capacidades de equipo de usuario final.

c. Separación de entornos de prueba y producción

- La dependencia encargada del Proceso de Tecnologías de Información debe separar los ambientes de pruebas y producción con el fin de reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.
- La dependencia encargada del Proceso de Tecnologías de Información debe garantizar los recursos necesarios que permitan la separación de los ambientes de pruebas y producción.

Artículo No. 23: Protección contra códigos maliciosos

a. Controles contra códigos maliciosos

Teniendo en cuenta que cada uno de los equipos de la Institución cuenta con una licencia de antivirus y un agente instalado en cada una de ellas, se debe:

- Todo el personal y terceras partes deben contar con un antivirus actualizado en sus dispositivos personales tales como: portátiles o celulares, si desean ingresar a la red de datos de la Institución.
- Todo el personal y terceras partes deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus instalado en los equipos por la dependencia encargada del Proceso de Tecnologías de Información.
- Todo el personal del TRA debe verificar, mediante el uso del software de antivirus, que todo archivo, independiente de su procedencia, esté libre de virus antes de ser accedido.
- Ninguna persona funcionaria del TRA debe descargar software desde sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la dependencia encargada del Proceso de Tecnologías de Información.
- Toda persona funcionaria y tercero que sospechen de alguna infección por virus deben dejar de usar inmediatamente el equipo de cómputo y notificar a la dependencia encargada del Proceso de Tecnologías de Información, para la revisión y eliminación del virus.
- Las personas funcionarias y terceros no deben realizar modificaciones o eliminar las configuraciones de seguridad en Antivirus, Outlook, software de ofimática, navegadores Web u otros programas, para detectar y prevenir la propagación de virus.
- Las personas funcionarias y terceros no deben intentar eliminar los virus de los equipos, a menos que sean personal autorizado por la dependencia encargada del Proceso de Tecnologías de Información, para garantizar la limpieza total de los equipos.

Artículo No. 24: Copias de respaldo

a. Copias de respaldo de la información

- El TRA, tiene el compromiso de la generación de copias de respaldo y almacenamiento de su información confidencial, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.

- Las áreas o dependencias propietarias de la información, con el apoyo de la dependencia encargada del Proceso de Tecnologías de Información, serán las encargadas de la generación de las copias de respaldo, se definirá la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.
- Asimismo, la dependencia encargada del Proceso de Tecnologías de Información se velará porque los medios que contienen respaldos de información crítica para la Institución sean almacenados en una ubicación diferente a las instalaciones donde se encuentra disponible. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

b. Política para realizar copias de respaldo de la información

Para una correcta realización y seguridad de los respaldos se deberán tener en cuenta estos puntos:

- La dependencia encargada del Proceso de Tecnologías de Información debe contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder realizar una reinstalación en caso de sufrir un percance. El procedimiento debe ser congruente con los requisitos de continuidad de las operaciones del TRA y formar parte de los procedimientos de continuidad de las tecnologías de información.
- La dependencia encargada del Proceso de Tecnologías de Información debe determinar los medios y herramientas correctos para realizar los respaldos, teniendo en cuenta los espacios necesarios, tiempos de lectura escritura, tipo de respaldo a realizar, etc.
- La dependencia encargada del Proceso de Tecnologías de Información debe realizar el almacenamiento de los respaldos en lugares diferentes de donde reside la información principal. De este modo se evita la pérdida total si hay un desastre que afecte todas las instalaciones de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información debe verificar la integridad de los respaldos que se están almacenando, de acuerdo con el procedimiento de revisión periódica de estos, con el fin de asegurar que al momento de requerir restaurar alguno de ellos funcione como se espera.
- Los jefes o encargados de proceso deben identificar la información que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.
- La dependencia encargada del Proceso de Tecnologías de Información debe contar con un procedimiento adecuado para garantizar la integridad física de los respaldos, en previsión de robo, destrucción o pérdida.
- La dependencia encargada del Proceso de Tecnologías de Información debe provisionar equipos de hardware con características similares a los utilizados para el

proceso normal de la operación del TRA, en condiciones necesarias para entrar en funcionamiento en caso de desastres físicos.

- Los jefaturas o encargados de proceso, para el caso de la información crítica para la ejecución su proceso y alojada en sus equipos, deben realizar el respaldo diario de las modificaciones efectuadas y guardar respaldos históricos semanalmente de dicha información mediante los mecanismos o herramientas proporcionadas por la dependencia encargada del Proceso de Tecnologías de Información.
- Las jefaturas o encargados de proceso como propietarios de los recursos tecnológicos y sistemas de información deben definir en conjunto con la dependencia encargada del Proceso de Tecnologías de Información, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.
- La dependencia encargada del Proceso de Tecnologías de Información debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios, esto para tener un plan de contingencia y poner en práctica, de alguna manera, la continuidad del negocio.

Artículo No. 25: Registro y seguimiento de eventos de los sistemas de información

El TRA, realizará monitoreo permanente del uso que dan las personas funcionarias a los recursos de la plataforma tecnológica y los sistemas de información de la Institución. Además, velará por la custodia de los registros o pistas de auditoría (de los sistemas de información) cumpliendo con los períodos de retención establecidos para dichos registros. Para esto se debe considerar los siguientes puntos:

- La dependencia encargada del Proceso de Tecnologías de Información, en conjunto con los responsables de los servicios, definirán la realización de monitoreo de las pistas de auditoría sobre los aplicativos donde se opera los procesos de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.
- La dependencia encargada del Proceso de Tecnologías de Información debe habilitar las pistas de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- La dependencia encargada del Proceso de Tecnologías de Información en conjunto con las personas responsables deben certificar la integridad y disponibilidad de las pistas de auditoría generadas en la plataforma tecnológica y los sistemas de información. Estos registros deben ser almacenados y sólo deben ser accedidos por personal autorizado.

Artículo No. 26: Control de software operacional

a. Instalación de software en sistemas operativos

- EL TRA, por medio de la dependencia encargada del Proceso de Tecnologías de Información, designará responsables y establecerá procedimientos para controlar la instalación de software en los equipos informáticos, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software sea actualizado.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer responsabilidades y procedimientos para controlar la instalación del software en los equipos de cómputo.
- La dependencia encargada del Proceso de Tecnologías de Información debe asegurarse que las aplicaciones desarrolladas por terceros realicen las respectivas pruebas antes de salir a producción.
- La dependencia encargada del Proceso de Tecnologías de Información debe asegurarse que el software instalado en la plataforma tecnológica cuenta con soporte preciso en caso de ser necesario y con los proveedores según sea requerido.
- La dependencia encargada del Proceso de Tecnologías de Información debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software, así como monitorear dichas actualizaciones.
- La dependencia encargada del Proceso de Tecnologías de Información debe validar los riesgos que genera la migración hacia nuevas versiones del software.
- La dependencia encargada del Proceso de Tecnologías de Información asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software es actualizado.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer las restricciones y limitaciones para la instalación de software en los equipos de cómputo.

Artículo No. 27: Gestión de vulnerabilidades

- El TRA, por intermedio de la dependencia encargada del Proceso de Tecnologías de Información, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de

pruebas de vulnerabilidades (al menos una vez al año), con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Este ejercicio podrá ser realizado con el apoyo de un tercero o servicio contratado.

- La dependencia encargada del Proceso de Tecnologías de Información debe generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

a. Restricciones sobre la instalación de software

- La dependencia encargada del Proceso de Tecnologías de Información debe realizar la instalación de software en los computadores suministrados por el TRA.
- La dependencia encargada del Proceso de Tecnologías de Información debe autorizar el software adicional que se requiera instalar en equipos de cómputo específicos del TRA.
- La dependencia encargada del Proceso de Tecnologías de Información mantendrá una lista actualizada del software autorizado y que se instalar en los computadores del TRA.

Artículo No. 28: Consideraciones sobre auditorías de sistemas de información

a. Controles sobre auditorías de sistemas de información

- El TRA, a través del Proceso de Auditoría Interna, verificará el cumplimiento de la política de seguridad, lo dispuesto en ente manual, la normatividad legal vigente y los requisitos propios de la organización cada año o según sea necesario.
- La dependencia encargada del Proceso de Tecnologías de Información debe planificar para reducir al mínimo las interrupciones de los procesos, de acuerdo con los requisitos de auditoría y las actividades relacionadas con la verificación de los sistemas operativos.

CAPÍTULO IX:
SEGURIDAD DE LAS COMUNICACIONES

Artículo No. 29: Políticas de Gestión de la seguridad de redes

El TRA por medio de la dependencia encargada del Proceso de Tecnologías de Información, establecerá los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios tecnológicos que soportan la operación de ésta; asimismo, velará por que se tengan los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se envía a través de dichas redes de datos.

De igual manera, proporcionará el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información interna y confidencial de la Institución.

- La dependencia encargada del Proceso de Tecnologías de Información debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red.
- La dependencia encargada del Proceso de Tecnologías de Información debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- La dependencia encargada del Proceso de Tecnologías de Información debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios y/o ubicación.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la Institución, acogiendo buenas prácticas de configuración segura, solicitarlos por escrito a los proveedores de servicio cuando aplique.
- La dependencia encargada del Proceso de Tecnologías de Información debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos en la red de datos del TRA e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- La dependencia encargada del Proceso de Tecnologías de Información debe instalar protección entre las redes internas y cualquier red externa, que esté fuera de la capacidad de control y administración de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos del TRA.

Artículo No. 30: Política de uso de la mensajería electrónica

En el TRA deberán aplicarse los siguientes controles para asegurar los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones por medio del correo electrónico, entendido la importancia de este servicio para la facilitación de la comunicación en la Institución.

- La dependencia encargada del Proceso de Tecnologías de Información debe diseñar y divulgar las normas para el uso de los servicios de correo electrónico.
- La dependencia encargada del Proceso de Tecnologías de Información debe garantizar que la plataforma de correo tenga los procedimientos y controles necesarios que permitan detectar y proteger la integridad de la información que viaja a través de esta plataforma.
- La dependencia encargada del Proceso de Tecnologías de Información debe asegurar que los mensajes electrónicos están protegidos contra código malicioso y pudiera ser transmitido a través de estos.
- La dependencia encargada del Proceso de Tecnologías de Información en conjunto con la dependencia encargada del Proceso de Gestión del Recurso Humano debe generar campañas de concientización a todo el personal respecto a las precauciones que deben adoptar en el intercambio de información confidencial y de uso interno por medio del correo electrónico.
- Todo el personal debe saber que la cuenta de ac electrónico asignada es de carácter individual; por consiguiente, ningún funcionario, en ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Las jefaturas o encargados de procesos deben designar responsables para la administración de las cuentas institucionales (cuando éstas apliquen), donde estas personas responderán por las mismas.
- Todo el personal debe utilizar el correo electrónico para envío de mensajes e información relacionada con el desarrollo de las labores y funciones asignadas a cada usuario. Ninguna persona funcionaria debe utilizar el correo electrónico institucional para actividades personales de ninguna índole, entre otras, el envío de cadenas de mensajes de cualquier tipo ya sea comercial, político, religioso, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los miembros de la Institución.
- El personal debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones, puesto que los mensajes e información contenida en los buzones de correo son propiedad del TRA.
- El personal y terceros no deben enviar archivos que contengan extensiones ejecutables con contenido malicioso, en ninguna circunstancia.

- El personal debe respetar el estándar de formato e imagen institucional definidos por el TRA para los mensajes electrónicos y deben conservar en todos los casos el mensaje legal de confidencialidad incluido en el pie de los correos electrónicos.

Artículo No. 31: Política de uso adecuado de Internet

Conscientes de la importancia de Internet como una herramienta para el desempeño de las labores diarias, el TRA proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades en la Institución.

a. La dependencia encargada del Proceso de Tecnologías de Información debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
b. La dependencia encargada del Proceso de Tecnologías de Información debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
c. La dependencia encargada del Proceso de Tecnologías de Información debe monitorear continuamente el canal o canales del servicio de Internet, en cuanto a carga y tráfico.
d. La dependencia encargada del Proceso de Tecnologías de Información debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
e. La dependencia encargada del Proceso de Tecnologías de Información debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
f. La dependencia encargada del Proceso de Tecnologías de Información en acompañamiento de la dependencia encargada del Proceso de Gestión Recursos Humanos campañas para concientizar al personal y terceros, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.
g. El personal y terceros deben hacer uso del servicio de Internet que provee el TRA para las actividades que guarden relación con su labor dentro de la Institución.
h. El personal debe abstenerse de descargar no autorizado desde internet, así como su instalación en las estaciones de trabajo asignados para el desempeño de sus labores, a menos que sean autorizados por la dependencia encargada del Proceso de Tecnologías de Información.

i. El personal y terceros no deben acceder a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y cualquier otra página que vaya en contra de la ética y la moral, las leyes vigentes del país o las políticas establecidas en este documento, a menos que la labor que tiene en el TRA, así lo requiera.
j. El personal no debe utilizar el servicio de Internet para el acceso y uso de servicios interactivos o mensajería instantánea como Facebook y otros similares, con el fin de intercambiar información confidencial o de uso interno de la Institución o para actividades que no corresponden con el desempeño de las funciones asignadas.
k. El personal y terceros no deben descargar, usar, intercambiar o instalar juegos, música, películas, información que de alguna manera atenten contra la propiedad intelectual de sus autores.
l. El personal y terceros no deben ejecutar archivos o herramientas que atenten contra la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica de la Institución. Entre ellas software no autorizado, archivos ejecutables desde medios extraíbles USB, ejecución de programas desde sitios web no autorizados, utilerías de sistema descargadas de Internet y que no son propietarias del sistema operativo. Ante dudas o sospecha del software a ejecutar, el personal deberá consultar con la Dependencia encargada del Proceso de Gestión de TI.
m. El personal y terceros deben asegurarse de que la información audiovisual (videos e imágenes) descargada y utilizada para las labores diarias no atenten contra la propiedad intelectual de sus autores.
n. El personal no debe intercambiar de ninguna forma, información confidencial para la Institución sin la debida autorización.
o. El uso de las redes sociales personales y el uso de YouTube o cualquier otro sitio que sea para visualizar videos que no sean para uso estrictamente laboral están prohibidas y bloqueadas salvo aquellos casos que sean aprobados por el Órgano Colegiado en que el uso de estas plataformas tecnológicas sea necesario para aquellos procesos o funcionarios que realmente sean de indispensable necesidad utilizarlos para la gestión de sus actividades laborales.

Artículo No. 32: Política de transferencia de la Información

Serán requeridas Políticas y procedimientos de transferencia de información ya que el TRA asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio.

- La Asesoría Legal, con el criterio técnico de la dependencia encargada del Proceso de Tecnologías de Información, debe definir los modelos de Acuerdos de Confidencialidad y de intercambio de información entre la Institución y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir:
    a. La prohibición de divulgar la información entregada por parte del TRA a los terceros con quienes se establecen estos acuerdos.
    b. La destrucción de dicha información una vez cumpla su cometido.

  Estos Acuerdos de Confidencialidad y de intercambio de información deben ser aprobados por el Órgano Colegiado.
- Previo a la ejecución de un contrato y conceder a un tercero acceso a información del TRA, la Asesoría Legal debe establecer en estos contratos los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de la Institución
- La dependencia encargada del Proceso de Tecnologías de Información debe velar porque el intercambio de información con entidades externas se realice en cumplimiento de este Manual de Políticas de Seguridad, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.
- El personal debe utilizar únicamente los mecanismos y herramientas proporcionadas por la dependencia encargada del Proceso de Tecnologías de Información para el envío o recepción de información confidencial para la Institución.
- El personal no debe revelar o intercambiar información confidencial de la Institución por ningún medio, sin contar con la debida autorización.

CAPÍTULO X:
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Nota: En este apartado del manual de política se asume que el TRA no desarrolla productos de software con recurso humano de la dependencia encargada del Proceso de Tecnologías de Información. Por tanto, únicamente se enlistan las prácticas de control que debe implementar esta dependencia para gestionar software desarrollado y/o adquirido por terceros.

Artículo No. 33: Políticas para establecer los requisitos de seguridad de los sistemas de información

El TRA asegurará que el software adquirido y desarrollado por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos y acordados para la solución. Las áreas propietarias de sistemas de información y la dependencia encargada del Proceso de Tecnologías de Información, incluirán requisitos de seguridad en la definición de requerimientos y posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido. Para ello se aplicarán los siguientes elementos:

- La dependencia encargada del Proceso de Tecnologías de Información debe aprobar la compra de los aplicativos o el software en concordancia con la política y/o procesos de adquisición de bienes y servicios de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, cuando así esta dependencia lo requiera.
- Las áreas propietarias de los sistemas de información, en acompañamiento con la dependencia encargada del Proceso de Tecnologías de Información debe, deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando los requerimientos de seguridad de la información.
- Las áreas propietarias de los sistemas de información deben definir qué información confidencial puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
- Los proveedores o terceros que desarrollen un sistema de información deben proporcionar los respectivos manuales, como son:
    a. Manual del usuario que describa los procedimientos de operación.

b. Manual técnico que describa su estructura interna, programas, catálogos y archivos.

Artículo No. 34: Seguridad en los procesos de desarrollo y de soporte

Se debe velar por un ambiente de desarrollo seguro. Por esta razón se deben implementar los siguientes aspectos.

- El TRA velará porque el desarrollo externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software adquirido cuente con el nivel de soporte requerido por la Institución. Este aspecto debe incluirse en los carteles de contratación cuando así se requiera.
- La dependencia encargada del Proceso de Tecnologías de Información en conjunto con los propietarios de los aplicativos debe realizar las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción.
- La dependencia encargada del Proceso de Tecnologías de Información en conjunto con los propietarios de los aplicativos debe realizar las pruebas de los sistemas de información utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción.
- La dependencia encargada del Proceso de Tecnologías de Información en conjunto con los propietarios de los aplicativos debe realizar las pruebas por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- La dependencia encargada del Proceso de Tecnologías de Información en conjunto con los propietarios de los aplicativos debe aprobar las migraciones entre los ambientes de pruebas y producción de sistemas de información nuevos y de cambios o nuevas funcionalidades.
- La dependencia encargada del Proceso de Tecnologías de Información debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La dependencia encargada del Proceso de Tecnologías de Información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.

- La dependencia encargada del Proceso de Tecnologías de Información debe asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- La dependencia encargada del Proceso de Tecnologías de Información debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- La dependencia encargada del Proceso de Tecnologías de Información debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información debe certificar el cierre de la conexión a las bases de datos desde los aplicativos y/o terceros tan pronto como estas no sean requeridas.
- La dependencia encargada del Proceso de Tecnologías de Información debe proteger el código fuente de las aplicaciones construidas, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

Artículo No. 35: Datos de prueba

En el TRA se protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción. Para ello:

- La dependencia encargada del Proceso de Tecnologías de Información debe certificar que la información entregada a los desarrolladores para realizar sus pruebas no revelará información confidencial de los ambientes de producción.
- La dependencia encargada del Proceso de Tecnologías de Información debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

CAPÍTULO XI:
SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

El TRA establecerá mecanismos de control en sus relaciones con los proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

El Órgano Fiscalizador debe incluir los requisitos de este capítulo que apliquen en los carteles de contratación.

Artículo No. 36: Política de seguridad de la información para las relaciones con proveedores

- La dependencia encargada del Proceso de Tecnologías de Información y la Asesoría Legal definen la siguiente cláusula de confidencialidad para la relación con proveedores:
  - ✓ El contratista y su personal deberán comprometerse a manipular y procesar todos los datos institucionales dentro de un ámbito de discreción, privacidad e integridad, de acuerdo con las políticas de control y seguridad institucionales. En ninguna circunstancia el contratista podrá utilizar información derivada de este trabajo para propósitos no contemplados en los procedimientos normales de desarrollo del servicio solicitado. El contratista deberá mantener contratos de confidencialidad con el personal que será destacado en el proyecto. La utilización indebida o negligente de los recursos institucionales, por prácticas imputables al contratista, serán consideradas factores de incumplimiento de la contratación y objeto de las sanciones administrativas y penales correspondientes.
- La dependencia de la Proveeduría Institucional y Asesoría Legal, deberán verificar que el cartel de contratación incluya la cláusula de Confidencialidad definida en el punto anterior, en los siguientes tipos de contrato:
  - ✓ Servicios de Soporte o mantenimiento de las aplicaciones existentes o nuevas aplicaciones del TRA. (Software)
  - ✓ b) Servicios de soporte o mantenimiento de los servidores del TRA (Hardware) o nuevos servidores.
  - ✓ c) Servicios de soporte o mantenimiento de la infraestructura de RED del TRA o nuevos equipos de red.
  - ✓ d) Servicios de soporte o mantenimiento de internet y telefonía IP o nuevos servicios de internet o telefonía ip.

- ✓ e) Servicios de soporte o mantenimiento de: Cámaras de seguridad (CCTV), aire acondicionado, Sistema de alimentación ininterrumpida (UPS), Sistema de Monitoreo de Edificio (BMS), sistema de iluminación del edificio, control de acceso al edificio (tarjetas), audio y video de salas del TRA, sistemas de control de incendios.

- Le corresponde al Órgano Fiscalizador de la contratación, asegurar que personal provisto por terceros o contratistas y que debido a sus funciones deban tener acceso a información del TRA. Será obligación del contratista presentar, ante el Administrador de la Contratación, dentro de los ocho (8) días hábiles siguientes a la notificación del Contrato por medio de SICOP una carta enviada a su personal asignado al servicio en la cual se compromete al cumplimiento de la cláusula de confidencialidad. Lo mismo aplicara cada vez que se cambia de personal durante la ejecución de lo contratado.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Institución.
- La dependencia encargada del Proceso de Tecnologías de Información debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica.

Artículo No. 37: Gestión de la prestación de servicios de proveedores

- El TRA velará por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con éstos. Asimismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.
- La dependencia encargada del Proceso de Tecnologías de Información debe verificar el momento pertinente para que el proveedor realice la conexión, apegándose a las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Institución.

CAPÍTULO XI:
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Artículo No. 38: Gestión de incidentes y mejoras en la seguridad de la información

Todos los incidentes de seguridad serán reportados por las personas funcionarias utilizando el medio o canal que haya dispuesto y comunicado la dependencia encargada del Proceso de Tecnologías de Información.

Cuando amerite la gestión de incorporación de nuevas políticas o directrices para minimizar riesgos, la dependencia encargada del Proceso de Tecnologías de Información presentará a la Comisión de Seguridad de la Información, un reporte de incidentes relacionado con la seguridad de la información.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Comisión de Seguridad de la Información será la única autorizada para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas. Aplicarán las siguientes responsabilidades y procedimientos.

- Las jefaturas o encargados de área como dueños de los activos de información deben reportar a la dependencia encargada del Proceso de Tecnologías de Información los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- La dependencia encargada del Proceso de Tecnologías de Información) debe evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares y escalar aquellos en los que se considere pertinente.
- La dependencia encargada del Proceso de Tecnologías de Información) debe reportar los incidentes a la Comisión de Seguridad instancia en la cual se debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad

reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su ocurrencia nuevamente.

- La dependencia encargada del Proceso de Tecnologías de Información debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
- El personal y terceros deben reportar cualquier evento o incidente relacionado con la seguridad de la información y los recursos tecnológicos con la mayor prontitud posible.
- El personal y terceros deben informar, en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno o confidencial, a la dependencia encargada del Proceso de Tecnologías de Información, para que se registre y se le dé el trámite necesario.

CAPÍTULO XII:
CUMPLIMIENTO

Artículo No. 39: Cumplimiento de requisitos legales y contractuales

El TRA velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ellas las disposiciones emitidas la Ley de Derechos de Autor y Conexos, razón por la cual la Auditoría Interna anualmente revisa que el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

a. Identificación de la legislación aplicable y de los requisitos contractuales

- La Asesoría Legal y la dependencia encargada del Proceso de Tecnologías de Información deben identificar, documentar y mantener actualizado un inventario de los requisitos legales, reglamentarios o contractuales aplicables a la Institución y relacionados con seguridad de la información. El inventario debe considerar para cada requisito legal un registro que contengan la referencia de la normativa, la(s) cláusula(s) aplicable(s), los impactos para el TRA y el responsable principal de la implementación del requisito o regulación.
- La dependencia encargada del Proceso de Tecnologías de Información debe certificar que todo el software que se ejecuta en la Institución esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- El personal no debe instalar software en sus estaciones de trabajo suministrados para el desarrollo de sus actividades sin la autorización de la dependencia encargada del Proceso de Tecnologías de Información a menos que su labor así lo requiera, acogiéndose al buen uso y licenciamiento del software que se está utilizando.
- El personal y terceros deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software sin la autorización del propietario de los derechos de autor y su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

b. Privacidad y protección de información de datos personales

En cumplimiento de la de Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley 8968 del 05 de setiembre de 2011), por la cual se dictan disposiciones para la protección de datos personales, el TRA velará por la protección de los datos personales de las personas funcionarias, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales el TRA como responsable de los datos personales obtenidos en sus distintos canales, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la Institución, hayan suministrado datos personales.

Asimismo, buscará proteger la privacidad de la información personal de las personas funcionarias estableciendo los controles necesarios para preservar aquella información que la Institución conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la actividad sustantiva y no sea publicada, revelada o entregada a las personas funcionarias o terceras partes sin autorización.

- Las áreas que procesan datos personales de funcionarios, de las personas funcionarias del TRA y terceros deben obtener la autorización expresa para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Institución.
- Las áreas que procesan datos personales de las personas funcionarias y usuarios los servicios del TRA y terceros, deben asegurar que solo aquellas personas que aceden a los datos tengan una relación laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de funcionarios, usuarios de los servicios del TRA y terceros deben acoger las directrices técnicas y procedimientos establecidos para enviar mensajes por correo electrónico a dichos usuarios.
- La dependencia encargada del Proceso de Tecnologías de Información debe establecer los controles para el tratamiento y protección de los datos personales de los funcionarios, usuarios de los servicios del TRA y terceros de los cuales reciba y administre información almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación, sin la autorización requerida.
- El personal debe guardar la discreción correspondiente o la reserva absoluta con respecto a la información de la Institución o de sus funcionarios de la cual tengan conocimiento en el ejercicio de sus funciones.

- El personal debe verificar la identidad de todas aquellas personas a quienes se les entrega información por teléfono, por correo electrónico o certificado, entre otros.
- Los usuarios que se registren en los sistemas de información del TRA deben aceptar un consentimiento informado del suministro de datos personales confirmando a su vez que la Institución puede delegar el tratamiento de estos datos a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información.

Artículo No. 40: Cumplimiento de requisitos legales y contractuales

Para asegurar el cumplimiento con las políticas de seguridad de la Información, la dependencia encargada del Proceso de Tecnologías de Información tiene como una de sus funciones proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para salvaguardar la información digital y física, los equipos de cómputo e instalaciones de cómputo, así como de las bases de datos de información automatizada en general.

a. Identificación de la legislación aplicable y de los requisitos contractuales

- La persona encargada de la Seguridad de la Información en conjunto con la dependencia encargada del Proceso de Tecnologías de Información debe gestionar la verificación del cumplimiento del Manual de Políticas de Seguridad de la Información.
- La dependencia encargada del Proceso de Tecnologías de Información puede implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo. El mal uso de los recursos informáticos que sea detectado será reportado.
- Las jefaturas o encargados de proceso como dueños de la información deben apoyar las revisiones del cumplimiento de las políticas de seguridad de la información que les competa y cualquier otro requerimiento de seguridad.

b. Identificación de la legislación aplicable y de los requisitos contractuales

El personal del TRA y terceros no deben hacer uso de herramientas de hardware o software para violar los controles de seguridad de la Información, a menos que se autorice por la dependencia encargada del Proceso de Tecnologías de Información.

- Ningún miembro del personal o tercero debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por la dependencia encargada del Proceso de Tecnologías de Información.
- Ningún miembro del personal o tercero debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a los equipos de cómputo, redes o información de la Institución.
- Ningún miembro del personal o tercero debe hacer uso de los recursos asignados para actividades no relacionadas con el propósito de la Institución, o bien con la extralimitación en su uso.
- Ningún miembro del personal o tercero debe realizar actividades como: traer equipos o ejecutar aplicaciones que no estén directamente especificados como parte del software, hardware o de los estándares de los recursos informáticos propios de la Institución.
- Ningún miembro del personal o tercero debe introducir en los Sistemas de Información o la red contenidos obscenos, amenazadores, inmorales u ofensivos.
- Ningún miembro del personal o tercero debe introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño a la información o los recursos informáticos.
- Ningún miembro del personal o tercero debe intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Ningún miembro del personal o tercero debe albergar datos de carácter personal en carpetas diferentes a la asignada para este fin, en los computadores de trabajo.
- Cualquier archivo introducido en la red o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.