Justicia	**Guía**	Código: **G-IC-14**
	Política de seguridad de la información	Versión: **005**
		Fecha de Vigencia: **2024-12-26**

Tabla de Contenido

1 OBJETIVO

El objetivo de este esta política es establecer los lineamientos generales de Seguridad de la Información del Ministerio de Justicia y del Derecho (en adelante MINJUSTICIA), para la toma de decisiones que afectan la confidencialidad, integridad y disponibilidad de la Información de la Entidad, basados en el marco legal y normativo teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información de MinTIC (en adelante MSPI).

2 ALCANCE

La Política de Seguridad de la Información aplica para los procesos estratégicos, misionales, de apoyo y evaluación del mapa de procesos de MINJUSTICIA, la implementación se realiza de manera gradual y su aplicación cubre:

• Información física o digital generada u obtenida por la entidad en el cumplimiento de su misión.
• Los colaboradores de la entidad, es decir funcionarios y contratistas directos.
• Personal externo vinculado a través de contratos con terceros, proveedores, visitantes, partes interesadas.

Las directrices están basadas en los lineamientos del MSPI de MinTIC y en la buena práctica de la Norma Técnica ISO 27001 vigente.

3 GLOSARIO

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y

recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).
Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
Autenticidad: Propiedad de que una entidad es lo que afirma ser.(ISO /IEC 27000)
Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. (ISO /IEC 27000)
Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Custodio de activos de información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.
Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma ISO 27001.
Disponibilidad: Propiedad de la información de ser accesible y utilizable a solicitud de una entidad autorizada. (ISO /IEC 27000)
E**ncargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
I**nformación Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
Integridad: Propiedad de la información relativa a su exactitud y completitud. (ISO /IEC 27000)
Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.
Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
M**ecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
MSPI (Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información de MinTIC): El Modelo de Seguridad y Privacidad de la Información - MSPI, conceptualizado y presentado por MINTIC imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.
No repudio: Capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades de origen. (ISO /IEC 27000).
Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
P**rivacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar, y la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
Propiedad intelectual (Dirección Nacional de Derechos de Autor, Unidad Administrativa Especial Ministerio del Interior): Se refiere a la protección del producto del intelecto humano, sea en los campos científicos literarios, artísticos o industriales. Esa protección concede a los

creadores, autores e inventores un derecho temporal para excluir a los terceros de la apropiación de conocimiento por ellos generados.
Proyecto: Se denomina proyecto al conjunto de actividades desarrolladas con el fin de alcanzar un objetivo, dichas actividades se interrelacionan y desarrollan de forma planeada y coordinada, el termino proyecto hace referencia a la planificación o con creación de un grupo de acciones que serán desarrolladas y al conjunto de recursos que serán usando para llevar a cabo el desarrollo y cumplimiento de objetivos concretos.
Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
Sistema de Gestión de Seguridad de la Información (en adelante SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
Teletrabajo (teletrabajo.gov.co): De acuerdo con la Ley 1221 de 2008 es "una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC - para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo".
Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
Tratamiento de riesgos: Proceso para modificar el riesgo. El tratamiento del riesgo puede involucrar lo siguiente; evitar el riesgo al decidir no comenzar o continuar con la actividad, tomar o aumentar el riesgo buscando una oportunidad, eliminar el riesgo, cambiar la probabilidad, cambiar las consecuencias, compartir el riesgo o retener el riesgo. (ISO /IEC 27000).
Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4 DESARROLLO

4.1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

“El Ministerio de Justicia y del Derecho, en el ejercicio de sus deberes con el Estado y los ciudadanos, declara su compromiso de implementar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información -SGSI, con el fin de proteger la confidencialidad, integridad y disponibilidad de sus activos de información, en cumplimiento de los requisitos legales y en concordancia con la misión y visión de la entidad”.

Esta política se revisa anualmente y se actualiza según las necesidades. En consecuencia, en atención a la creación de cultura y conciencia de seguridad de la información, debe ser conocida y

cumplida por todos los colaboradores y demás partes interesadas que hagan uso de los activos de información de la entidad.
El incumplimiento de las políticas se considerará un incidente de seguridad, podrá dar lugar a un proceso disciplinario para los funcionarios y se convertirá en una causa válida de terminación del contrato con los contratistas, o aliados a través de acuerdo o convenio vigente. Así mismo, dependiendo del caso habrá sanciones pecuniarias o penas de prisión de acuerdo con la Ley 1273 de 2009.

4.2 OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Justicia y del Derecho establece los siguientes objetivos generales de la gestión de seguridad de la información en el marco de la Política, los cuales se encuentran alineados con los objetivos estratégicos de la Entidad:

1. Apropiar el Modelo de Seguridad y Privacidad de la Información, para proteger los activos de información de MINJUSTICIA respecto a las características de confidencialidad, integridad y disponibilidad.
2. Mitigar los riesgos de seguridad de la información con el establecimiento de controles para proteger la información de la entidad, con base en la normatividad aplicable y los lineamientos del Gobierno Nacional.
3. Atender oportunamente los incidentes de seguridad de la información, identificando sus causas para implementar acciones correctivas, en el marco de mejora continua del SGSI.
4. Cumplir con el marco legal y regulatorio del MINJUSTICIA en cuanto a los aspectos aplicables a la seguridad de la información, teniendo en cuenta el cumplimiento de la Ley de Protección de Datos Personales y la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
5. Establecer, promover y mantener la cultura en seguridad y privacidad de la información entre los colaboradores de la entidad y del sector justicia.

4.3 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.3.1 ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los roles que se tendrán establecidos para la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) se basan en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.
En el nivel táctico se encuentran el Comité Institucional de Gestión y Desempeño y el/la Responsable de Seguridad de la Información designado por la entidad. En el nivel operativo se encuentra un equipo con diferentes roles relacionados con la seguridad y finalmente, como participantes tenemos a las partes interesadas.
Las partes interesadas como la ciudadanía, entidades adscritas y entes de control interno y externo pueden conocer y realizar algún tipo de seguimiento o veeduría, dentro del alcance de sus funciones, en cuanto al cumplimiento normativo en el Sistema de Gestión de Seguridad de la Información. Los proveedores y aliados deberán acogerse a las políticas definidas por la entidad, en el marco de la relación contractual o convenio con la entidad.

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

En el marco de la Resolución 1939 de 2019 el Comité Institucional de Gestión y Desempeño del MINJUSTICIA hará las veces de Comité de Seguridad de la Información, contando entre sus funciones con la de: Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.
Así mismo, la Resolución 254 de 2018 establece que la Política de Seguridad Digital es liderada por la Subdirección de Tecnologías y Sistemas de Información, en el Marco del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Política de Gobierno Digital, la cual debe ser transversal en el Ministerio de Justicia y del Derecho.
El (La) Señor(a) Ministro(a), los Viceministros, Secretario General, Directores, Subdirectores, Jefes de Oficina y Coordinadores de Grupo deben conocer y promulgar las políticas de seguridad de la información del Ministerio, promoviendo su cumplimiento entre funcionarios y contratistas a su cargo, con el fin de aunar esfuerzos de toda la organización para el cumplimiento de la política y objetivos del SGSI.

RESPONSABLE U OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

El/La Responsable u Oficial de Seguridad de la Información y Seguridad Digital es el rol encargado de planear, orientar y realizar control y seguimiento de actividades encaminadas al fortalecimiento de la seguridad de la información, y demás acciones definidas en el marco de los planes para la implementación, mantenimiento y mejora continua del SGSI de MINJUSTICIA. El Subdirector de Tecnologías y Sistemas de Información ejercerá este rol, a menos que se cuente con un Oficial de Seguridad de la Información en la entidad. Dado que se trata de una entidad cabeza de sector, también es el designado como enlace sectorial de seguridad digital, de acuerdo con el Manual Operativo de MIPG.

Sus responsabilidades son:
• Fomentar la implementación de la Política de Seguridad Digital.
• Asesorar a la entidad, liderar, coordinar y controlar el avance en la planeación, implementación, mantenimiento y mejora del SGSI de la Entidad.
• Definir, revisar y actualizar mínimo una vez al año las políticas de seguridad de la información del MINJUSTICIA.
• Definir, proponer e implementar los procedimientos o documentos que sean de su competencia para la operación del SGSI.
• Identificar la brecha entre el Modelo de Seguridad y Privacidad de la Información de MinTIC y la situación actual de la entidad.
• Diseñar y ejecutar, en el marco de la estrategia de uso y apropiación de TIC, un plan y/o estrategia de comunicación, sensibilización y divulgación en seguridad de la información, con el fin de promover la adecuada protección de los activos de información de la entidad.
• Liderar y brindar acompañamiento a los procesos y proyectos de la entidad en la gestión de riesgos de seguridad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
• Mantener informada a la Alta Dirección, a través del Comité Institucional de Gestión y Desempeño sobre los avances del SGSI e informar igualmente irregularidades, incidentes o prácticas que atenten contra la seguridad de la información de acuerdo con la normativa vigente.
• Articular con las entidades adscritas del Sector Justicia los elementos estratégicos y operativos de seguridad de la información que permitan incrementar el nivel de madurez en cada una de ellas.

EQUIPO DE INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD INFORMÁTICA

• Establecer los controles, medidas técnicas y administrativas necesarias para proteger la infraestructura tecnológica, los sistemas y los activos de información de MINJUSTICIA.

• Evaluar, emitir conceptos y avalar las nuevas soluciones o plataformas tecnológicas a adquirir o implementar en la Entidad, teniendo en cuenta el cumplimiento de los requisitos de seguridad de la información.
• Analizar, evaluar y seleccionar herramientas y servicios que faciliten la labor de seguridad informática para su implementación en la entidad.
• Gestionar los riesgos y eventos de seguridad informática y su registro, solución y/o escalamiento interno y externo con autoridades y entes competentes en articulación con el/la Responsable u Oficial de Seguridad de la Información, de conformidad con la normatividad vigente.
• Verificar y controlar la implementación de controles de seguridad informática sobre las plataformas tecnológicas del Ministerio, de acuerdo con las políticas y evaluaciones de riesgos generadas en el marco del SGSI.
• Para el cumplimiento de estas responsabilidades, se cuenta con el equipo de ingenieros encargados de las plataformas tecnológicas de la Entidad.
• Liderar la protección de los recursos lógicos, de los datos que se procesan, almacenan o transmiten a través de la infraestructura tecnológica de MINJUSTICIA, así como la correcta utilización de los servicios de Internet, correo electrónico y herramientas colaborativas; realizando el monitoreo, detección y reporte de anomalías.
• Gestionar un inventario actualizado de la infraestructura crítica de la Entidad, incluyendo los proveedores y partes interesadas externas que interactúan con dicha infraestructura.

EQUIPO DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con la guía de roles y responsabilidad del MSPI de MinTIC, debe conformarse un equipo, con el propósito hacer seguimiento y control de los avances en la implementación del Modelo de Seguridad y Privacidad de la información MSPI. En el Ministerio de Justicia y del Derecho; el equipo que continuamente está apoyando la gestión de la seguridad de la información está conformado por:
• Director de Tecnologías y Gestión de Información en Justicia
• Subdirector(a) de Tecnologías y Sistemas de Información
• Subdirector(a) de Gestión de Información en Justicia
• Oficial de Seguridad de la información (si se cuenta con la persona, de lo contrario lo ejerce el Subdirector de Tecnologías)
• Líder de infraestructura tecnológica
• Coordinador de mesa de ayuda
• Líder de sistemas de información
• Líder de calidad de TI

Este equipo tiene la responsabilidad de apoyar al Responsable u Oficial de Seguridad de la Información en la implementación, mantenimiento y mejora del SGSI, asesorando y resolviendo las dudas técnicas y de procedimiento que se generen durante la gestión.
Adicionalmente, se encuentra delegada en la Subdirección de Tecnologías y Gestión de Información la función de liderar la implementación de la Política de Protección de Datos Personales, labor que debe alinearse con el SGSI de la entidad, en el marco del MSPI.
Finalmente, las diferentes dependencias de la entidad deben aunar esfuerzos para apoyar el SGSI, en especial el equipo de talento humano, gestión contractual, gestión jurídica y control interno, de acuerdo al alcance de sus responsabilidades o funciones.

4.3.2 CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS ESPECIAL

La STSI y en particular el Responsable u Oficial de Seguridad de la Información deben mantener contacto y tener comunicación con las autoridades y grupos de interés especial como foros y

asociaciones, así como entidades líderes en temas de ciberseguridad y ciberdefensa con el fin de alinear la gestión del SGSI y para la solución de los incidentes de seguridad de la información (ColCERT, CSIRT, MinTIC, CCOC, Policía Nacional, Fiscalía, etc.).
El Grupo de Gestión Administrativa debe mantener los contactos con empresas de servicios públicos de energía y agua, servicios de emergencias como el cuerpo de bomberos y la Policía Nacional, para reportar y atender situaciones imprevistas de seguridad física o suministro de servicios. La STSI administra los contactos con los proveedores de bienes y servicios de telecomunicaciones, soporte y mantenimiento de infraestructura tecnológica, para la atención de incidentes.

4.3.3 SEGURIDAD DE LA INFORMACIÓN EN LA GESTION DE PROYECTOS

Se deben incluir y tener en cuenta todos los lineamientos y políticas de seguridad de la información en la gestión de proyectos de la entidad, en la medida que involucren activos de información y posibles impactos en la integridad, disponibilidad y/o confidencialidad de los mismos.
El supervisor del contrato, jefe inmediato o quien haga el seguimiento del proyecto es el responsable de incluir la seguridad de la información e integrar los métodos que se tengan definidos para la gestión de proyectos del Ministerio de Justicia y del Derecho, con el fin de asegurar que los riesgos y controles de seguridad de la información sean identificados y tratados como parte del proyecto a ejecutar.
Los métodos de control que se requieren para la gestión de los proyectos son:
- Establecer la matriz de riesgos para el proyecto.
- Los objetivos de la política de seguridad de información serán incluidos en el proyecto a ejecutar.
- En la etapa inicial del proyecto se deberá realizar la viabilidad y valoración de riesgos de seguridad de la información para la identificación de los controles de seguridad que se ejecutarán en el desarrollo del mismo.
- La política de seguridad de la información deberá cumplirse a lo largo de la totalidad de las fases de la metodología aplicada en el proyecto a ejecutar.
- Se debe especificar los roles encargados de revisar de manera regular las implicaciones de seguridad de la información que se hayan definido en la metodología de gestión del proyecto en ejecución.
- Se debe liderar la planeación, ejecución y seguimiento del proyecto a ejecutar, teniendo en cuenta los requisitos de seguridad de la información. Esta actividad se llevará a cabo por parte del equipo o persona designada en la entidad como gerente o encargado de dicho proyecto.
- El supervisor del contrato y/o jefe inmediato debe asegurar que la transferencia de información y/o conocimientos asociados al desarrollo del proyecto sean documentados en su totalidad a fin de llevar seguimiento en caso de cambio del recurso humano.
- Para el caso de los contratos con personas jurídicas se debe realizar seguimiento sobre los riesgos tecnológicos incluidos en la matriz de riesgos de los estudios previos y/o pliego de condiciones.

4.3.4 ACTIVOS DE INFORMACIÓN

INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
En cumplimiento de las obligaciones legales y contractuales, MINJUSTICIA identifica los activos de información, los dueños y custodios, así como las responsabilidades asociadas a la gestión de los mismos.

Se elabora y aprueba el inventario de activos de información tipo dato, del cual se obtiene el registro de activos de información, así como el índice de información clasificada y reservada de MINJUSTICIA, en cumplimiento de la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional – Ley 1712 de 2014. Esta información se complementa con el inventario de hardware, personas o roles, software e instalaciones críticos de cada proceso. Adicionalmente, se cuenta con los catálogos de sistemas de información e infraestructuras tecnológicas a cargo de la Subdirección de Tecnologías y Sistemas de Información y del inventario específico de equipos de cómputo elaborado por la dependencia a cargo de la Gestión de Almacén e Inventarios de la entidad.
El inventario consolidado de activos de información contiene la identificación de los activos, su clasificación (en términos de confidencialidad, integridad y disponibilidad) y valor para la entidad; así como el responsable de la dependencia a cargo de cada uno de los activos (rol denominado "propietario" en las guías de MinTIC) y los custodios para cada uno de ellos. Este inventario de activos será actualizado al menos una vez al año, en cumplimiento del procedimiento P-IC-06 Gestión de activos de información. Los instrumentos de gestión de la información pública derivados del inventario de activos serán aprobados bajo el acto administrativo correspondiente, dando cumplimiento a la normatividad.
El propietario o responsable de los activos de información de cada una de las dependencias debe velar por que se lleve a cabo la validación y seguimiento del cumplimiento de los controles de seguridad definidos en la matriz de riesgos los cuales se establecen para mitigar los riesgos identificados y asociados a cada uno de los activos, así como de los planes de tratamiento que se hayan definido por parte de la dependencia.
De acuerdo con la clasificación de los activos de información en cuanto a su confidencialidad, dada por la información clasificada y/o reservada que contengan y en aplicación de la normatividad, los procesos de gestión documental, gestión de vulnerabilidades técnicas, gestión de incidentes, políticas de TIC y procedimiento de gestión de acceso a recursos informáticos, los responsables de las dependencias a cargo de los activos deben definir y revisar periódicamente los permisos de acceso a los mismos, los cuales serán aplicados por los administradores de los sistemas de información o custodios.

USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS

Los responsables de los activos de información de cada dependencia tienen los siguientes compromisos:

• Mantener actualizado el inventario de activos de información.
• Promover la confidencialidad de la información contenida en los activos categorizada como clasificada y/o reservada, según lo previsto en la normatividad vigente.
• Delegar los custodios para cada activo según sus competencias y las funciones correspondientes a su cargo.
• Controlar el cumplimiento de las responsabilidades relativas a los activos de información, por parte de los custodios designados.
• Realizar de manera periódica la validación y seguimiento del cumplimiento de los controles de seguridad definidos en la matriz de riesgos los cuales se establecen para mitigar los riesgos identificados.
• Definir y revisar periódicamente las restricciones y clasificaciones de acceso a los activos, teniendo en cuenta las políticas de control de acceso aplicables.
• Promover el manejo apropiado del activo cuando es eliminado o dado de baja, de acuerdo con la normatividad vigente, las políticas y procedimientos de gestión de bienes y las tablas de retención documental de la Entidad.
• Gestionar con la STSI la custodia, protección y copias de respaldo de los activos de información digitales y electrónicos.

• Gestionar con el grupo de gestión documental la custodia y protección de los activos de información físicos.
Los custodios de los activos de información (es decir, quienes mantienen bajo su responsabilidad, información u otros activos de los cuales no son los propietarios) tienen la responsabilidad de gestionar la aplicación de los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de los activos de información; en el marco de las políticas de Seguridad de la información del MINJUSTICIA y en cumplimiento de la Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, Ley 1581 de 2012 de Protección de Datos Personales, así como cualquier otra normativa que las reglamente, reforme, modifique o adicione.
Los custodios de la información alojada en la infraestructura tecnológica ubicada en el Data Center de MINJUSTICIA, tienen bajo su responsabilidad gestionar la implementación de los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de los activos de información. Los componentes tecnológicos estarán bajo la administración de los equipos de infraestructura y de sistemas de información de la STSI.

Lo anterior sin perjuicio de la responsabilidad de la Subdirección de Tecnologías y Sistemas de Información, de aplicar los controles de seguridad informática definidos en las políticas de: seguridad de la información, tratamiento y protección de datos personales, tecnologías y gestión de la información, así como en los planes de tratamiento de riesgos que permiten hacer un uso responsable de los accesos privilegiados a los sistemas de información y los datos. Se pueden presentar casos en los cuales los activos de información como las bases de datos de sistemas de información y portales sean custodiadas técnicamente por parte de dicha Subdirección, lo cual implica la prestación de los servicios tecnológicos de administración, soporte, mantenimiento y copias de respaldo de las bases de datos. Sin embargo, la gestión de los controles, identificación y clasificación de los activos, así como la calidad de la información será responsabilidad de los propietarios y custodios de los activos de la(s) dependencia(s) que, de acuerdo con sus funciones, deba(n) gestionarlos.

La STSI administra los repositorios seguros de información que incluyen los esquemas de backup establecidos. Las áreas que requieran espacios adicionales deben realizar la solicitud a través de la mesa de Ayuda de TI. La STSI realiza copias de respaldo a la información que se encuentra alojada en los servidores del Data Center. No se realizan respaldos de información individual alojada en nube -la cual está disponible según los acuerdos de nivel de servicio contratados-, ni de la información alojada en los equipos de cómputo, la cual es responsabilidad del usuario.
Los activos de información que pertenecen o están bajo la gestión de MINJUSTICIA deben utilizarse exclusivamente con propósitos funcionales en el marco de la misionalidad y la estrategia institucional, en concordancia con la ética y en cumplimiento de la normatividad y políticas internas vigentes.
No se debe guardar información personal en ninguno de los recursos tecnológicos o equipos de cómputo suministrados por el MJD. La utilización de los recursos de la entidad para manejo de información personal se realiza bajo la responsabilidad de cada colaborador y la STSI no se hace responsable ni debe garantizar el acceso a plataformas de correo personal, pasarelas de pago, aplicaciones de trasferencia de información, bancos o entidades financieras. En cumplimiento de las políticas de seguridad la STSI tiene la potestad de bloquear los accesos a este tipo de sitios web.
Para el uso aceptable de activos de hardware, software y en general recursos tecnológicos, consultar la Política de Tecnologías y de Gestión de la información G-IC-17, documento publicado dentro del Sistema Integrado de Gestión –SIG de la DTGIJ.

DEVOLUCIÓN DE ACTIVOS, ETIQUETADO Y TRANSFERENCIA DE INFORMACIÓN

En el evento en que se dé por terminada la relación contractual o laboral con el MJD o se presente un cambio de cargo, rol, funciones o un traslado a otra dependencia de la Entidad, los

colaboradores deben realizar la devolución formal de los activos de información que han sido asignados o que se encontraba gestionando en virtud de sus funciones o actividades a cargo, de conformidad con los procesos de Gestión de Recursos Informáticos y de Administración del Talento Humano vigentes al finalizar la relación de intercambio de información, relación laboral o contractual.

Los proveedores y terceros que manejen activos de información de la entidad deben realizar un borrado seguro cuando finalice la relación contractual o convenio de intercambio de información, tal como lo describen los formatos de confidencialidad de información.

CONTROL DE TRANSFERENCIA DE LA INFORMACIÓN

En el evento que se necesite generar, compartir o enviar copias de activos con información clasificada o reservada a otras dependencias o entes externos, en el desarrollo de las funciones de la Entidad y con observancia de la normatividad aplicable, el responsable de la dependencia a cargo del activo debe advertir sobre la naturaleza de dicha información, etiquetarla o marcarla y garantizar que se haya realizado la firma de acuerdo o compromiso de confidencialidad con el tercero. Adicionalmente, tanto el propietario del activo como su custodio deben velar porque se intercambie información únicamente a través de canales seguros, como VPN, plataformas propias o de terceros, FTP seguro, etc. No se remitirán a entes externos activos con datos personales o sensibles, que hayan sido identificados como información clasificada o reservada, a menos que se haya destinado el canal seguro aprobado por la STSI y se cuente con la autorización del propietario de los mismos.
Se establece y se debe cumplir con el procedimiento para intercambio seguro, el cual busca la protección de la información en el momento de ser transferida o intercambiada con las otras entidades y establece los controles necesarios para el intercambio de información.
El Grupo de Gestión Documental define los procedimientos requeridos para la trasferencia documental interna y con terceras partes y garantiza la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones; en el marco de la normatividad legal vigente. Dicha dependencia debe asegurar que el envío de información física a terceros (documentos o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por MINJUSTICIA, los cuales permitan ejecutar rastreo de las entregas.

ACUERDOS DE TRANSFERENCIA DE INFORMACIÓN

Los acuerdos interadministrativos de intercambio de información se realizarán de acuerdo con lo establecido en el Procedimiento para el intercambio de información P-IC-03. En caso de que no se suscriba minuta de convenio de intercambio de información con las entidades, se deberá realizar el diligenciamiento del formato de acuerdo o compromiso de confidencialidad establecido por la gestión contractual, a menos que se intercambie únicamente información pública.
Los propietarios de los activos de TI, o a quienes ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega y recepción.

Así mismo, los responsables o propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información de MINJUSTICIA a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
Los terceros con quienes se intercambia información de MINJUSTICIA, deben darle manejo adecuado a la información recibida, en cumplimiento de las políticas de seguridad de la Entidad, de las condiciones contractuales establecidas y previo diligenciamiento del acuerdo o compromiso de confidencialidad.

4.3.5 GESTIÓN DE ACCESOS E IDENTIDADES

SEGREGACIÓN DE FUNCIONES

En la definición de los procesos y procedimientos de la entidad, así como en la gestión de los accesos a los sistemas de información y recursos informáticos, se debe asegurar que los deberes y áreas de responsabilidad en conflicto se encuentren segregados.
En el Manual Especifico de Funciones y Competencias Laborales de MINJUSTICIA, el cual es aprobado, adicionado y modificado por acto administrativo, así como en los documentos en los cuales se especifican las obligaciones de los contratistas de prestación de servicios, se asignan los diferentes roles y responsabilidades, de acuerdo con el perfil del colaborador. Adicionalmente, la estructura organizacional de la entidad presenta las funciones, responsabilidades y nivel jerárquico de cada dependencia y cargo dentro de la misma.
Es responsabilidad del líder de cada proceso y responsable de los activos, asegurar que ninguno de los colaboradores pueda registrar, modificar y autorizar una transacción financiera o actividad operativa que pueda generar la materialización de riesgos de gestión, corrupción o de seguridad de la información. Se deben segregar en diferentes grupos, dependencias y/o personas las etapas de registro, aprobación, tratamiento y custodia de los activos tipo información.

CONTROL DE ACCESO

La administración de los usuarios en las redes de datos, servicios tecnológicos y sistemas de información que contemple la creación, modificación, bloqueo o inactivación de cuentas de usuario, debe realizarse a través de la STSI o los administradores autorizados por parte de las áreas funcionales. Toda solicitud de creación, modificación o novedad de usuarios debe realizarse en cumplimiento del procedimiento P-TI-02 Gestión de acceso a recursos informáticos, a menos que se trate de un sistema de información bajo la administración de un área funcional. En ese caso, los administradores deben llevar registro de las asignaciones y perfiles aprobados, solicitar la correspondiente autorización del jefe inmediato o supervisor de contrato y en caso de entidades externas, validar el convenio y/o acuerdo de intercambio con el MJD.

Para realizar la creación de las cuentas de usuario se debe tener en cuenta las primeras tres letras del nombre seguido de las primeras tres letras del apellido, en caso de contar con homónimos se agrega al final del primer apellido la letra del segundo apellido o en caso de aplicar se tomará el segundo nombre como referencia.

El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario será responsabilidad de la persona a la cual le fue asignado. El control de trabajo remoto, así como el tiempo de uso del acceso VPN por parte de los colaboradores, se podrá restringir únicamente a los horarios de oficina. Todos los accesos a los servicios tecnológicos deben tener vigencia de uso. Para los contratistas de prestación de servicios, debe corresponder con la fecha de terminación del contrato.
La asignación de usuario tipo administrador local del equipo debe ser asignado únicamente en casos excepcionales para los colaboradores que lo requieran previa autorización y validación de la STSI; se llevara un registro digital de las autorizaciones concedidas para acceder a un equipo con perfil de administrador local junto con su justificación y autorización.

La STSI a través de la Mesa de Ayuda debe asegurarse de que los usuarios que ingresen por primera vez a los servicios del MINJUSTICIA realicen el cambio de contraseña de acceso. Se deben aplicar mecanismos de verificación de identidad del usuario antes de reemplazar la información sensible para la autenticación o proporcionar una nueva o temporal, a través de la Mesa de Ayuda de MINJUSTICIA.

MANEJO DE CONTRASEÑAS

La STSI debe asegurar que las contraseñas para el ingreso a los servicios tecnológicos de la entidad no sean visibles en texto claro.

Las contraseñas de acceso a servicios tecnológicos deben cumplir con las siguientes características mínimas de complejidad:

- Tener mínimo ocho (8) caracteres alfanuméricos.
- Para el servicio VPN se debe tener un mínimo seis (6) caracteres.
- Usar una combinación entre mayúsculas, minúsculas, números y caracteres especiales [¡”#$%&/()@*_+?¿><.,]
- No ser ninguna palabra o fecha asociada a su persona (nombre de la entidad, país, nombres de mascotas o de familiares, o fecha de nacimiento o fecha del año actual)
- Las contraseñas no deben iniciar con un número, deben iniciar por una letra ya sea mayúscula o minúscula.
- No se puede repetir las últimas cinco contraseñas utilizadas.

Lo anterior debe asegurarse, en la medida de lo posible, de manera automática a través del directorio activo y los módulos de gestión de usuarios de los sistemas de información y plataformas que no se autentiquen directamente a través de directorio.
La STSI debe implementar políticas de seguridad que garanticen el cambio de las contraseñas por parte de los usuarios de forma periódica para el ingreso a los servicios tecnológicos administrados por dicha dependencia.

POLÍTICA DE ACCESO A SERVICIOS DE RED

La STSI es responsable de las redes de datos y los servicios de red de MINJUSTICIA, por lo tanto, debe velar por que estas se encuentren debidamente protegidas contra accesos no autorizados implementando controles de acceso lógico. Toda solicitud de creación, modificación, bloqueo o eliminación de usuarios de acceso a los servicios de red a través de VPN, debe realizarse a través de la Mesa de Ayuda.

La conexión remota a la red de área local de MINJUSTICIA debe ser establecida a través de una conexión VPN segura, aprovisionada por la STSI. Los usuarios serán responsables de evitar el acceso desde equipos y conexiones a través de redes públicas que no cuenten con las medidas de seguridad estipuladas y validadas por la STSI.
La STSI debe asegurar que las redes inalámbricas de MINJUSTICIA cuenten con métodos de autenticación que eviten accesos no autorizados, así como el cambio de contraseña de manera periódica. Se deben implementar controles para evitar que los equipos ajenos a la entidad accedan a la red local de la entidad.

POLÍTICA DE SEGURIDAD DE USUARIOS PRIVILEGIADOS

La STSI gestiona y administra las plataformas de red, correo, seguridad perimetral, filtrado de contenido (proxy), ofimática y debe otorgar los privilegios para la administración de los servicios tecnológicos, solo a aquellos colaboradores designados para dichas funciones.
La STSI debe garantizar que los usuarios y contraseñas de usuario que traen por defecto los sistemas operativos, el firmware, las bases de datos y demás elementos tecnológicos sean

cambiados o suspendidos de acuerdo con las políticas y las mejores prácticas de seguridad. Así mismo, se cambiarán periódicamente y en especial, cuando se presenten modificaciones de personal asignado. Se implementarán herramientas para asegurar el Múltiple Factor de Autenticación, en especial para estas cuentas de acceso privilegiado. Los administradores deberán tener acceso a las plataformas a través de una cuenta diferente a la de usuario final.

CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y APLICATIVOS

La STSI junto con las áreas funcionales y administradoras de los sistemas de información y aplicaciones, debe velar por que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, así mismo debe ejecutar mecanismos para que los desarrolladores, tanto internos como externos, acojan las buenas prácticas de desarrollo seguro en los productos generados, con el fin de controlar el acceso lógico y evitar accesos no autorizados cuando estos estén en producción.

La STSI debe establecer ambientes separados a nivel físico y lógico para pruebas y producción; contando con su plataforma, servidores, aplicativos, dispositivos y versiones independientes de los otros ambientes, para evitar así que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad, confidencialidad y disponibilidad de la información de los servicios en producción.
La STSI debe promover los controles necesarios, que los usuarios utilicen diferentes perfiles, es decir que las personas responsables de los ambientes pruebas y no tengan acceso a producción y así mismo que los menús muestren los mensajes de identificación apropiados para reducir el riesgo de error.
La STSI debe establecer los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe promover que los desarrolladores internos y externos, posean acceso controlado a los datos y archivos que se encuentren en los ambientes de producción. Adicionalmente, debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
MINJUSTICIA debe establecer niveles de intervención y autoridad sobre los sistemas de información para garantizar que los sistemas se usen de manera segura y efectiva. Esto se deberá definir en los requerimientos técnicos o en el manual de usuario de cualquier software construido o contratado, deberá realizarse en un trabajo colaborativo entre la Dirección de Tecnologías y Gestión de Información en Justicia y el Área Funcional encargada del proceso o software.
Los niveles de intervención y autoridad para los sistemas de información deben incluir lo siguiente:

- **Nivel técnico**: El nivel técnico se centra en los detalles y la implementación de los sistemas informáticos. Los colaboradores en este nivel son responsables del diseño, la implementación y el mantenimiento de los sistemas informáticos. También son responsables de la resolución de problemas y el soporte técnico.

- **Nivel táctico:** El nivel táctico se centra en el uso de los sistemas informáticos para apoyar los objetivos de la organización. Los colaboradores en este nivel son responsables de desarrollar e implementar estrategias de TI que apoyen las operaciones institucionales. También son responsables de gestionar los recursos de TI y asegurar que los sistemas estén cumpliendo con los requisitos de la organización.

- **Nivel operativo:** El nivel operativo se centra en el uso diario de los sistemas informáticos. Los usuarios en este nivel son responsables de ingresar datos, generar informes y usar los sistemas de información de manera eficiente.

El área funcional debe asignar la responsabilidad de cada nivel de intervención y autoridad a un colaborador o equipo específico y es responsable de asegurar que el sistema de información se use de manera consistente con los requisitos MINJUSTICIA. Así mismo, debe informar a la DTGIJ cada vez que haya un cambio o una asignación de rol o responsabilidad de los niveles técnico o táctico sobre el sistema de información. La Dirección de Tecnologías del MJD revisará y aprobará el cambio o la asignación antes de que se implemente.
Los administradores y custodios de los servicios de información y aplicaciones deben autorizar el acceso a sus sistemas de información o aplicativos de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos. Es responsabilidad de las áreas funcionales y administradoras de los sistemas de información el monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos. Los desarrolladores deben promover que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas. Los desarrolladores deben asegurar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

RESPONSABILIDAD DE LOS USUARIOS

Los usuarios deben mantener la confidencialidad de la información de autenticación a los servicios tecnológicos de MINJUSTICIA. Es responsabilidad del colaborador realizar el cambio de contraseña cuando solicite su renovación por olvido o mínimo una vez cada 45 días, una vez la contraseña caduque el sistema forzará su modificación.

En caso de que el usuario crea que su contraseña ha sido comprometida por terceros, debe realizar el cambio inmediatamente e informar por medio de la Mesa de Ayuda a la STSI de la situación que se presenta.

4.3.6 SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON LOS PROVEEDORES

En el marco de los procesos precontractuales y contractuales, las áreas solicitantes deben asegurar la firma del F-GC-04-44 Formato Compromiso de Confidencialidad de Información – Contratistas por parte del representante legal del proveedor o aliado, documento en el cual se establecen las responsabilidades del tercero en materia de seguridad y privacidad de la información, así como el compromiso de no divulgación, cumplimiento normativo y de políticas de seguridad, siempre que, en la ejecución del contrato o convenio se tenga acceso, intercambie, consulte o manipule activos de información de MINJUSTICIA, que contengan o almacenen información pública clasificada o reservada.

Los supervisores de los contratos deben velar por que la información de MINJUSTICIA sea protegida de divulgación no autorizada, errores u omisiones en el tratamiento de la misma o incumplimientos normativos, legales o contractuales por parte de los terceros a quienes se entrega dicha información, verificando el cumplimiento de las cláusulas relacionadas en los contratos y los acuerdos o compromisos de confidencialidad y no divulgación firmados.
Adicionalmente, las áreas funcionales con necesidades de contratación de proveedores de bienes o servicios de tecnología, deben solicitar orientación y acompañamiento de la Dirección y Subdirección de Tecnologías de la Información con el fin de establecer y definir los requisitos técnicos, analizar la viabilidad y dar lineamientos para la definición de las obligaciones de seguridad de la información a cumplir por parte del tercero.
Se debe asegurar la gestión de riesgos de seguridad de la información relacionados con la cadena de suministro de productos y servicios de TIC, implementando los controles preventivos necesarios para mitigar la probabilidad de afectación a la entidad, por fallas, incumplimientos o errores de los proveedores. Para estos

terceros es indispensable la firma del formato de compromiso de confidencialidad, y se recomienda la inclusión de cláusulas contractuales o anexos al contrato relacionados con acuerdos de niveles de servicio que, en lo posible, generen descuento a factura en caso de incumplimiento, así como la existencia, documentación y cumplimiento de políticas de seguridad de la información y protección de datos personales y de un plan de contingencia de los productos y/o servicios contratados.
La validación del cumplimiento de los requisitos de seguridad por parte del tercero y/o proveedor se encuentra a cargo del área solicitante, con la asesoría de la Subdirección de Tecnologías y Sistemas de Información y el Responsable u Oficial de Seguridad de la Información.

SEGURIDAD PARA SERVICIOS EN NUBE

Al contratar servicios en la nube se debe revisar dónde se almacenarán los datos geográficamente y validar si ese país está aprobado por la Superintendencia de Industria y Comercio de Colombia, para la transferencia de datos personales, dadas las condiciones adecuadas para la protección de los mismos. El proveedor deberá garantizar la protección de la información gestionada y/o almacenada, en cuanto a su integridad, confidencialidad y disponibilidad. Se deberá exigir el cumplimiento de acuerdos de niveles de servicio para la atención y solución de incidentes de seguridad de la información que puedan afectar la información o la disponibilidad de servicios de MINJUSTICIA. En caso de órdenes de compra en la plataforma de compras del estado colombiano, estas condiciones estarán contempladas en el acuerdo marco y la STSI realizará seguimiento a su cumplimiento.

La STSI velará por mantener los controles de seguridad con base en las políticas, incluyendo reglas para proteger su contenido, plataformas, aplicaciones, sistemas y redes, del mismo modo que lo hace para las plataformas ubicadas en el centro de datos en sus propias instalaciones. Lo anterior incluye, pero no se limita a la encriptación de los activos con información clasificada y reservada, aplicar los controles de acceso con esquema de contraseñas seguras y múltiple factor de autenticación, verificar las configuraciones por defecto, cambiar las contraseñas iniciales de administración y mantener la gestión de software antivirus y antimalware.

4.3.7 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad de la información se realizará de acuerdo con el P-IC-04 Procedimiento Gestión de Incidentes de seguridad de la información a cargo de la STSI y del Responsable u Oficial de Seguridad de la Información.

El equipo de infraestructura tecnológica debe realizar frecuentemente un análisis del comportamiento de la red, idealmente mediante herramientas de monitoreo automático. El análisis debe incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones de red con que generan mayor tráfico, direcciones de red que reciben mayor número de peticiones, uso de VPN´s y los que considere necesarios con el fin de prevenir y detectar la posible ocurrencia de un incidente. Adicionalmente, se aplicarán los parches y últimas actualizaciones en sistemas operativos, servicios y aplicaciones; así como las recomendaciones del CSirt Gobierno, ColCert y otros organismos de ciberseguridad.

Adicionalmente, como parte de las actividades de prevención, en el marco de la estrategia de concientización y sensibilización de los colaboradores, se incluirán en especial los temas de Ciberamenazas, prevención en seguridad de la información y reporte de eventos e incidentes de seguridad a la STSI a través de un caso en Mesa de Ayuda de TI.
Los colaboradores, tienen la responsabilidad de reportar a través de un caso en el aplicativo a la Mesa de Ayuda de TI cualquier situación irregular que pueda tratarse de un evento o incidente de

seguridad de la información, como incumplimiento de las políticas y controles establecidos, uso inadecuado de los activos de información, correos sospechosos, etc.
La STSI debe evaluar todos los eventos de seguridad reportados a través de la Mesa de Ayuda de TI o detectados a través de los análisis y monitoreos realizados, de acuerdo con sus circunstancias particulares y escalar al Responsable u Oficial de Seguridad de la Información o quien haga sus veces aquellos que sean catalogados como incidentes (dado que se materializó un riesgo y se afectó la confidencialidad, integridad y/o disponibilidad de la información), para evaluar criticidad y definir acciones a tomar. Entre las medidas de respuesta y contención se encuentran el aislar equipos, detener servicios y deshabilitar cuentas de usuarios, entre otros. Si se considera necesario, se informará a los colaboradores, Alta Dirección y/o CoCERT o CSirt Gobierno, Policía Nacional, etc.
La STSI, con el apoyo del Responsable u Oficial de Seguridad de la Información o quien haga sus veces debe velar porque se apliquen buenas prácticas para la identificación, recolección, adquisición y preservación de evidencia, de acuerdo con los diferentes tipos de medios y dispositivos. Las lecciones aprendidas, una vez solucionados los incidentes, deben ser documentadas con el objetivo de aplicar los conocimientos adquiridos en el mejoramiento de los controles y prevención de nuevos incidentes de seguridad.

CONTINUIDAD DE NEGOCIO

MINJUSTICIA definirá documentará, divulgará y realizará pruebas de un Plan de Continuidad de Negocio de toda la organización, con el fin de establecer las estrategias de recuperación de los procedimientos críticos para la entidad, disminuyendo el impacto reputacional, operativo /o legal ante un evento que pueda afectar gravemente el normal funcionamiento de los procesos de la entidad. Como parte del PCN se definirán las estrategias necesarias para mantener unos niveles adecuados de seguridad de la información, previniendo que se pueda afectar la integridad y confidencialidad de la información crítica para MINJUSTICIA.

La STSI realizará la gestión necesaria para planificar, implementar y mantener la continuidad de los sistemas de información, portales web, equipos de telecomunicaciones y demás recursos tecnológicos críticos para el cumplimiento de la misionalidad de la entidad, ante un incidente grave; lo cual se logra a través de un Plan de Recuperación de Desastres diseñado, documentado, divulgado y probado. Se definirán así mismo, los controles mínimos requeridos para conservar la seguridad de los activos de información durante un desastre.

4.3.8 OTRAS POLITICAS ORGANIZACIONALES

REQUISITOS LEGALES, ESTATUTARIOS Y REGLAMENTARIOS

Se deben identificar, documentar y mantener actualizados los requisitos a cumplir parte de MINJUSTICIA en lo relacionado con la seguridad de la información. El Oficial u/o Responsable de Seguridad de la Información realizará la revisión de la normatividad, leyes, decretos, circulares y demás documentos emitidos por parte de los entes reguladores y de control con el fin de tomar acciones a través de los planes de seguridad y privacidad y plan de tratamiento de riesgos, para dar cumplimiento a los nuevos requisitos en materia de seguridad digital y de la información. La documentación se realizará a través del normograma actualizado de la entidad.

POLÍTICA DE DERECHOS DE AUTOR

MINJUSTICIA, en cumplimiento con el marco regulatorio de protección a la propiedad intelectual y los derechos de autor, evita, detecta y sanciona conductas encaminadas a la vulneración de los derechos de autor, que busquen el beneficio propio o para terceros de una obra o creación intelectual; así como actos u omisiones que induzcan a error a los colaboradores de la entidad, con la finalidad de obtener una ventaja financiera o de cualquier tipo, para evitar una obligación.

Para evitar el uso indebido de cualquier tipo de software o archivo de audio, digital o video que no esté debidamente licenciado, así como cualquier forma de uso indebido de las invenciones de carácter intelectual, el Ministerio vigila el incumplimiento de la Constitución, al Estatuto Anticorrupción o al Código Disciplinario, que puedan ser considerados como fraude o piratería.
La Alta Dirección del Ministerio es responsable por la administración, prevención y detección del riesgo de fraude y piratería, acompañando en todo momento las políticas establecidas por el Gobierno Nacional sobre el particular. Los colaboradores de la Entidad son responsables por evitar incurrir en alguna de estas conductas y denunciar su detección, en caso tal de tener conocimiento de las mismas. Así mismo, la Subdirección de Tecnologías y Sistemas de Información tiene a cargo la gestión del licenciamiento del software adquirido por la Entidad, de acuerdo con las políticas de seguridad de la información y de tecnologías de la información.

PROTECCIÓN DE REGISTROS Y DATOS PERSONALES

MINJUSTICIA debe asegurar la protección de los registros de información en formato físico, electrónico o digital para evitar su pérdida, destrucción, falsificación, revelación o acceso no autorizados. Con tal fin, se identifican los activos de información de la entidad, sus propietarios, custodios, tipo, formato, clasificación de criticidad y ubicación, lo cual se documenta en el inventario de activos de información, de acuerdo con el procedimiento P-IC-06 Gestión de activos de información. Los custodios de los activos son los responsables de la aplicación de los controles necesarios para proteger la información, de acuerdo con la gestión de riesgos de seguridad de la información.

Por otra parte, el Grupo de Gestión Documental establece, documenta y divulga las directrices para la gestión del archivo, referentes al almacenamiento, retención, protección y disposición final de los documentos de la organización. Adicionalmente, la STSI implementa los controles de seguridad informática sobre los repositorios oficiales de información, bases de datos de los sistemas, centro de datos y demás hardware e instalaciones de infraestructura critica a su cargo, para preservar la seguridad de los registros en formato digital o electrónico.
En cuanto a la gestión de los datos privados almacenados en las bases de datos, es esencial comprender las responsabilidades compartidas entre las áreas propietarias de los sistemas de información y la Subdirección de Tecnología y Sistemas de Información. Las áreas propietarias son las encargadas de asegurar que el tratamiento de estos datos cumpla con las normativas vigentes. Esto incluye la correcta clasificación, manejo y protección de los datos según las leyes y regulaciones aplicables.
Por otro lado, la Subdirección de Tecnología y Sistemas de Información tiene la tarea de custodiar la información, lo que implica mantener la seguridad de los datos y gestionar la programación de copias de seguridad de manera uniforme para todas las bases de datos según lo establecido en el procedimiento P-TI-04 “Respaldo y Restauración de los sistemas de Información”. Aunque la Subdirección se encarga de realizar y custodiar estas copias, es responsabilidad de las áreas propietarias definir las tablas de retención para dichas copias de seguridad. Esto significa que deben establecer los periodos durante los cuales las copias de seguridad deben ser conservadas antes de su eliminación o archivado definitivo. Esta colaboración asegura que los datos privados sean protegidos adecuadamente y que se cumplan los requisitos legales y de seguridad.

Para la protección de los activos de información que contienen datos personales, la Dirección de Tecnologías y Gestión de Información en Justicia, delegada por la Alta Dirección de MINJUSTICIA, lidera la implementación de la Política y el programa de protección de datos personales, transversal a toda la organización, dando cumplimiento a la Ley 1581 de 2012 y sus decretos reglamentarios.

CUMPLIMIENTO Y REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Todos los colaboradores de MINJUSTICIA deben conocer y dar cumplimiento a las políticas de seguridad de la información descritas en el presente documento y se podrán realizar revisiones periódicas de cumplimiento de las mismas, de manera independiente por parte de entes de control internos o externos. La DTGIJ, STSI y/o el Responsable u Oficial de Seguridad de la Información no serán, en ningún caso los responsables de la implementación y el cumplimiento de todas las políticas específicas que han sido definidas y documentadas.

La entidad está obligada a dar cumplimiento a los requisitos legales establecidos por el Gobierno Nacional y MinTIC dentro de la normatividad vigente aplicable, en el marco de la Política de Gobierno Digital, Política de Seguridad Digital y Modelo de Seguridad y Privacidad de la Información de MinTIC. Las normas técnicas y estándares internacionales aplicables a la ciberseguridad y la seguridad de la información serán implementadas en la medida de las posibilidades, como buenas prácticas, sin un carácter obligatorio.
En caso de que se presenten inconformismos con el cumplimiento de las políticas y los controles de seguridad por parte de los colaboradores de MINJUSTICIA, el funcionario, contratista o tercero que no acoja y decida no cumplir con la política y/o el control, afrontará las posibles consecuencias sobre la seguridad de los activos de información de la entidad.

PROCEDIMIENTOS OPERATIVOS DOCUMENTADOS

La STSI es responsable de documentar y/o mantener la documentación (entregada por terceros) necesaria para ejecutar las actividades asociadas con la gestión de los recursos tecnológicos, tales como la instalación y configuración de sistemas de información y plataformas, copias de respaldo de información, mantenimiento de equipos, gestión del data center, equipos de telecomunicaciones y centros de cableado, administración de plataforma de red, correo, seguridad perimetral, filtrado de contenido y suite ofimática, control de cambios, solución de incidentes tecnológicos, contactos de soporte y escalamiento, reinicio y actualización de sistemas, procedimientos de recuperación, gestión de logs de auditoría y monitoreo de red y plataformas críticas.

4.4 CONTROLES RELACIONADOS CON LAS PERSONAS

4.4.1 SELECCIÓN E INGRESO DEL PERSONAL, ACUERDOS DE CONFIDENCIALIDAD

El Grupo de Gestión Humana, así como el Grupo de Gestión Contractual, antes de realizar la vinculación, deben realizar las verificaciones necesarias para confirmar la veracidad de la

información suministrada en la hoja de vida del candidato y verificar los antecedentes penales de los candidatos seleccionados para hacer parte de la entidad.
El Grupo de Gestión Humana debe garantizar que los funcionarios firmen el F-TH-01-13 Formato Declaración de Títulos Académicos, Certificación de Políticas, uso y Autorización de Tratamiento De Datos Personales. el cual incluye el compromiso con el cumplimiento de la normatividad en cuanto al tratamiento de los datos personales (Ley 1581 de 2012) y la aceptación de Políticas de Seguridad de la Información. Este documento firmado debe ser guardado en la respectiva carpeta de hoja de vida del funcionario.
En el caso de los contratistas, proveedores y aliados, el Grupo de Gestión Contractual asegura la firma y el correcto diligenciamiento del F-GC-04-44 Formato Compromiso de Confidencialidad de Información - Contratistas el cual incluye el cumplimiento de la normatividad en el tratamiento de los datos personales (Ley 1581 de 2012) y la aceptación de Políticas de Seguridad de la Información. El formato firmado se debe guardar con el contrato o acuerdo en su respectiva carpeta, antes de iniciar sus actividades.

4.4.2 TÉRMINOS Y CONDICIONES DEL EMPLEO

Es responsabilidad del jefe Inmediato o Supervisor del contrato, informar las responsabilidades, actividades y tareas asignadas al nuevo personal antes de dar acceso a la información de propiedad de MINJUSTICIA.
Los colaboradores tienen prohibida la divulgación de información confidencial a la cual tengan acceso en cumplimiento de sus obligaciones y actividades, en cualquier contexto y sin autorización expresa y documentada de los responsables de los activos de información que contengan este tipo de información.
El personal provisto por terceros debe velar por el cumplimiento del acuerdo de confidencialidad y de la Política de Seguridad de la Información de la Entidad conforme al desarrollo de sus actividades. Así mismo, los terceros contratados por proveedores deben conocer y cumplir el compromiso de confidencialidad firmado por el proveedor con el Ministerio y cumplir con lo establecido en la Política de Seguridad de la Información.
Los directivos y jefes de oficina del MINJUSTICIA deben promover la importancia de la seguridad de la información entre colaboradores, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas de seguridad digital de la Entidad. Es responsabilidad de los colaboradores, informar de cualquier irregularidad que pueda considerarse un incidente de seguridad de la información a través de la Mesa de Ayuda de TI.
Es responsabilidad del Jefe Inmediato o quien este delegue, reportar licencias, vacaciones accesos a recursos informáticos (Sistemas de información, portales, correo electrónico, EPX, usuario de red, etc.). En el caso de la Mesa de Ayuda se debe especificar si se requiere suspensión, modificación, desactivación, configuración de respuesta automática o reenvío en el caso de correo electrónico.

4.4.3 CONCIENCIA DE SEGURIDAD DE LA INFORMACIÓN, EDUCACIÓN Y FORMACIÓN

El/La Responsable u Oficial de Seguridad de la Información debe diseñar y ejecutar de manera periódica una estrategia de concientización en seguridad de la información, con el fin de apoyar la protección adecuada de los activos de información, en el marco de la estrategia y planes de uso y apropiación de las TIC de MINJUSTICIA. Se contará con el apoyo de la Oficina de Prensa y Comunicaciones, así como del Grupo de Gestión Humana, para desarrollar las actividades de divulgación de información, sensibilización, capacitación y formación de los colaboradores de la entidad, con los recursos disponibles.

Con base en las necesidades detectadas, se solicitará incluir dentro del Plan Institucional de Capacitación la formación requerida para los funcionarios, en materia de seguridad y privacidad

de la información, de acuerdo con sus roles y responsabilidades dentro de la entidad.

Los colaboradores que hagan uso de la información de MINJUSTICIA, deben dar cumplimiento a las políticas, lineamientos y procedimientos de seguridad de la información, así como participar en las sensibilizaciones, capacitaciones y/o entrenamientos de seguridad de la información.

4.4.4 POLÍTICA DE TELETRABAJO Y TRABAJO REMOTO

MINJUSTICIA debe asegurar el cumplimiento de la normatividad vigente relacionada con el teletrabajo, incluyendo el aseguramiento del adecuado uso de las tecnologías de la información y las comunicaciones para los funcionarios que se encuentren trabajando bajo esta modalidad; así como las validaciones requeridas en materia de cumplimiento de políticas y controles de seguridad de la información y protección de datos personales.
La Subdirección de Tecnologías y Sistemas de Información deberá realizar las actividades necesarias para asegurar la configuración y validación de equipos de cómputo, recursos de comunicación y conectividad, así como establecer los mecanismos para proveer la conexión remota segura a los equipos y sistemas de información de la entidad, y a los medios de almacenamiento autorizados; de manera que se cuente con los controles necesarios para que se gestionen los activos de información de forma segura. Adicionalmente, la STSI velará porque se realice el monitoreo del uso de los recursos dispuestos para el teletrabajo, previniendo y conteniendo los incidentes de seguridad de la información por ataques cibernéticos u otras causas.
Los líderes de proceso y dueños de los activos de información deberán otorgar las autorizaciones requeridas para que los teletrabajadores ejerzan sus funciones desde su hogar, procurando que las labores que realicen no requieran el acceso directo a los activos de información con información clasificada y/o reservada. En caso de que así sea, el responsable de los activos deberá informar al funcionario de la responsabilidad que conlleva el manejo de la información confidencial en su equipo de trabajo desde casa y realizar un monitoreo constante al uso seguro de los recursos y accesos con los cuales cuenta el teletrabajador.
Los funcionarios en modalidad de teletrabajo deben realizar sus actividades únicamente desde los dispositivos de MINJUSTICIA o autorizados por la entidad, configurando el inicio de sesión exclusivo para su perfil de acceso. La información utilizada o generada durante su gestión en las instalaciones de la entidad y durante el teletrabajo, debe ser almacenada en los medios autorizados para ello (OneDrive, unidades compartidas y SharePoint corporativos) sin descargar, almacenar y guardar información en sus dispositivos personales, móviles, USB o discos duros extraíbles, a menos que cuenten para ello con la autorización de los líderes de proceso y propietarios de los activos, y que los mismos sean encriptados por parte del personal de la STSI.
Los funcionarios en teletrabajo deberán informar a la Mesa de Ayuda de TI sobre cualquier incidente o evento en el cual se sospeche o se conozca de incumplimiento a las políticas y controles de seguridad de la información o posible afectación de la confidencialidad, integridad o disponibilidad de los activos de la entidad (información, hardware, software). Igualmente, deben utilizar solamente la conexión autorizada por la STSI de MINJUSTICIA, sin transportar el equipo asignado a otras ubicaciones, como café internet, centros comerciales, etc y nunca hacer uso de las redes Wi-Fi públicas en lugares como los mencionados.

Los contratistas de prestación de servicios o personal vinculado por parte de proveedores, aliados u otras entidades, deben presentar sus equipos para revisión de la Mesa de Ayuda de TI en cuanto a licenciamiento y actualización de software, antivirus licenciado instalado y capacidad disponible, antes de asignarles y configurarles permisos para conexión remota a los recursos de la

entidad. Los equipos propios son responsabilidad del funcionario o contratista, quien debe cumplir con las políticas y controles establecidos por la entidad para su correcto uso y protección de los activos de la entidad.

4.4.5 PROCESOS DISCIPLINARIOS Y SANCIONES

Es deber de todos los colaboradores de MINJUSTICIA dar cumplimiento a las políticas contenidas en este documento, así como la Política de Protección y Tratamiento de Datos Personales y reportar por medio de un caso a Mesa de Ayuda de TI cualquier conducta sospechosa o incumplimiento a las políticas y controles, por parte de personal de la entidad o externos.
Adicionalmente, el colaborador debe poner en conocimiento de su jefe directo, Jefe del Grupo de Control Disciplinario Interno y/o el Responsable u Oficial de Seguridad de la Información o quien haga sus veces, así como de las autoridades pertinentes, cualquier evento sobre fraude, acceso abusivo a sistemas o piratería, para lo cual puede utilizar los diferentes canales de denuncia. El Ministerio protege los datos y la identidad del denunciante.
Cualquier tipo de infracción o incumplimiento de esta política será objeto de las acciones y sanciones legales pertinentes, las cuales se rigen conforme a los parámetros establecidos en Código Disciplinario Único, Código Penal y en el Código de Ética del MINJUSTICIA.

4.4.6 CAMBIOS O FINALIZACIÓN DE LA VINCULACIÓN

El Grupo de Gestión Humana debe monitorear y reportar dentro de los 5 días siguientes a la fecha en la que tenga conocimiento del retiro del servidor público, vacaciones, licencias, desvinculación o cambio de labores de los colaboradores a la STSI a través de la Mesa de Ayuda.
El supervisor de contrato o jefe inmediato debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los colaboradores a la STSI a través de la Mesa de Ayuda.
Es responsabilidad de los colaboradores utilizar los repositorios oficiales para el almacenamiento de la información y documentación producida y gestionada durante la vinculación con la entidad, así como realizar la entrega de la misma, una vez finalice el contrato con la Entidad. Es responsabilidad del Jefe Directo o Supervisor del Contrato verificar que esto se cumpla. Se deja el registro mediante la firma del formato F-TI-02-02 Certificación de Paz y Salvo Finalización de Contratos de Prestación de Servicios Profesionales y/o Apoyo a la Gestión.
La información de MINJUSTICIA se debe proteger, no se puede reproducir, usar o divulgar sin la debida autorización, durante la relación contractual y una vez finalizada la misma El jefe directo o supervisor de contrato debe verificar que los accesos a los sistemas de información y plataformas de la entidad se inhabiliten al finalizar el contrato. En caso de no ser así, es su responsabilidad afrontar las consecuencias derivadas de posibles casos de violación a la confidencialidad, integridad y disponibilidad de la información.

4.5 CONTROLES FÍSICOS

4.5.1 PERIMETRO DE SEGURIDAD, ENTRADA FÍSICA Y MONITOREO

MINJUSTICIA, a través de la gestión de la Secretaría General y el Grupo de Gestión Administrativa, debe velar por implementar los mecanismos de seguridad física y control de

acceso a las instalaciones, de manera que se asegure el perímetro de las instalaciones y se cuenta con las condiciones de seguridad adecuadas para proteger las instalaciones críticas de las amenazas que pueden comprometer la integridad, confidencialidad y disponibilidad de los activos (hardware, software, personas e indirectamente, activos tipo información).
Los perímetros de las oficinas, bodegas de archivo y demás instalaciones deben contar con pisos, techos y muros externos de construcción sólida, todas las puertas y ventanas al exterior deben ser protegidas contra accesos no autorizados con cerraduras, barras y deben estar bloqueadas cuando se encuentran desatendidas. Se debe monitorear cualquier acceso por medio de circuito cerrado de TV y alarmas. Se debe contar con un área de recepción, para validar y registrar el ingreso y salida del personal, tanto colaboradores como visitantes, así como los movimientos de computadores propios o de la entidad, entrada y salida de archivos físicos, para lo cual se debe contar con autorización del Grupo de Gestión Documental.

4.5.2 ASEGURAMIENTO DE OFICINAS E INSTALACIONES

Las áreas de procesamiento y almacenamiento de información, como el centro de datos, centro de conectividad, centros de cableado, archivo de gestión y bodega de archivo central, centro de monitoreo y vigilancia, así como las dependencias que manejan información crítica para la entidad, deben considerarse de acceso restringido y deben contar con controles adicionales para asegurar el ingreso de las personas autorizadas únicamente.

Es responsabilidad del líder de cada dependencia y propietario de los activos de información, gestionar la implementación de controles de acceso adicionales para proteger activos de información clasificada y reservada. Los mismos pueden consistir en aislamiento de la oficina, validación de datos, carnet y/o autorización especial para el ingreso de colaboradores y visitantes, puerta con acceso controlado por lector de huella, clave o sensor de proximidad.

4.5.3 PROTECCIÓN CONTRA AMENAZAS FÍSICAS Y AMBIENTALES

La Secretaría General, a través del Grupo de Gestión Administrativa o quien haga sus veces, debe asegurar que MINJUSTICIA cuente con las medidas necesarias de infraestructura y seguridad física para evitar daños causados por posible incendio, inundación, terremoto, explosión, desorden de orden público y otros desastres naturales o provocados. Esto aplica para los edificios de oficinas propios, rentados o en concesión que eventualmente se ocupen por parte del personal, bienes, infraestructura tecnológica o archivo pertenecientes a la entidad. En lo posible, debe contarse con instalaciones con diseño antisísmico, sistema de detección de incendios, alarmas, pólizas de seguros; así como un Plan de prevención, preparación y respuesta ante emergencias implementado, divulgado y probado, el cual está enmarcado dentro del Sistema de Gestión de Seguridad y Salud en el Trabajo de la entidad.
Por otra parte, tanto la STSI como el Grupo de Gestión Documental establecerán las medidas necesarias y realizará la gestión para solicitar su implementación, de manera que se logre proteger la infraestructura tecnológica y los archivos de gestión y central de las amenazas físicas y ambientales, como la corrosión, polvo, temperaturas extremas, humedad, plagas, fenómenos meteorológicos o desastres naturales, con el apoyo del Grupo de Gestión Administrativa, de manera que se implementen sistemas de monitoreo y control de condiciones ambientales como temperatura, humedad, plagas. En el caso del Grupo de Gestión Documental, estas medidas se incluyen dentro del Sistema Integrado de Conservación SIC.

4.5.4 TRABAJO EN ÁREAS SEGURAS

Las áreas de la entidad que se consideren “seguras” debido a la información u otros activos críticos que administran, deben estar aisladas del resto de la entidad y tener controles adicionales implementados, como ingreso autorizado y con registro, monitoreo a través de cámaras de

seguridad, trabajo supervisado, prohibir el uso de celulares, cámaras, esferos o algún otro dispositivo con el cual se pueda generar copias no autorizadas de la información. Para MINJUSTICIA aplica para el archivo de gestión centralizado por el Grupo de Gestión Documental y la bodega de archivo central, así como para el centro de datos y los centros de conectividad y cableado.

4.5.5 ESCRITORIO Y PANTALLA LIMPIOS

La entidad está comprometida con la protección de sus activos de información, para lo cual colaboradores, así como cualquier otro personal que labore en las instalaciones del Ministerio debido a las necesidades y con la debida autorización, debe dar cumplimiento a las siguientes medidas que están enfocadas en evitar o reducir la pérdida de información, manteniendo buenas prácticas de pantalla y escritorio limpios, en los lugares de trabajo.

- El colaborador o tercero con acceso a la información, no debe guardar información de la entidad en dispositivos móviles y/o personales, (USB, discos duros externos, PC y/o portátiles personales, tabletas, memorias, etc), la información debe estar almacenada únicamente en los repositorios dispuestos para ello: OneDrive, SharePoint y carpetas compartidas en servidores de archivos seguros y custodiados por la STSI. En caso excepcional de que se autorice por el propietario del activo la copia en unidades externas, estas deben ser cifradas por parte de la STSI, lo cual se solicitará por un caso a Mesa de Ayuda de TI.

- Para los activos de información críticos, los responsables o custodios de los mismos deben almacenar asegurar su almacenamiento en los repositorios oficiales con acceso restringido y se debe solicitar realizar el respaldo de la información a la STSI.
- Los documentos en papel y los dispositivos de almacenamiento removibles con información clasificada o reservada, como pueden ser unidades USBs, discos duros externos, CD, DVD, entre otros; deben ser almacenados apropiadamente en cajones o archivadores con llave, cuando no está siendo utilizados y todos los días, al finalizar la jornada laboral.
- Los archivadores, carpetas físicas, CDs, DVDs y otros medios removibles, en lo posible deben estar etiquetados, de manera que se pueda identificar el tipo de información contenida.
- Los recursos que forman parte del puesto de trabajo del colaborador deben estar organizados, en condiciones de fácil acceso y permanecer en buen estado. No debe quedar información expuesta, ni acumulación de documentos o papeles de trabajo.
- Sobre los escritorios de las oficinas y áreas de trabajo, cerca de los computadores o documentación impresa, no está permitido manejar líquidos ni comidas u otras sustancias que puedan ser derramadas y ocasionar daños.
- información clasificada o reservada deben recogerse inmediatamente de la impresora y la reproducción o fotocopiado de información con estos grados de confidencialidad deben ser conocidos y autorizados por los responsables y los custodios de los activos de información.
- Todos los usuarios de computadores de escritorio o portátiles deben bloquear la sesión cuando no los están usando (CTRL+ALT+SUPR o Tecla Windows + L). Para los computadores de la red del Ministerio, el protector de pantalla se activa automáticamente después de cinco minutos de inactividad. En caso de que no esté funcionando correctamente, el colaborador debe crear un caso a Mesa de Ayuda reportando dicha situación.
- Igualmente, los administradores de plataformas y aplicaciones deben asegurar el bloqueo por inactividad de las sesiones de VPN, escritorio remoto y acceso a los diferentes sistemas de información.
- En las pantallas de los computadores solamente deben estar los accesos directos a las aplicaciones más usadas. No se permite el almacenamiento de archivos o los accesos

directos a los mismos en el escritorio del computador. En caso de guardar información digital o electrónica local, esta debe ser almacenada de manera ordenada dentro de la carpeta “Documentos” del equipo de cómputo asignado, con nombres de archivos y subcarpetas que permitan identificar el tipo de información allí contenida.

- Los usuarios que manejen información clasificada o reservada no deben tener ubicado su computador cerca de una zona de tránsito de personal, en especial si es público o de otras dependencias. El equipo debe ser ubicado de manera que terceras personas no puedan ver la información de la pantalla.
- Las contraseñas de acceso a la red, correo, portales y sistemas de información son de uso personal e intransferible. Son confidenciales y por tal razón está absolutamente prohibido escribirlas en papeles, notas o documentos a la vista. La única excepción a esta medida lo constituyen las contraseñas de los usuarios genéricos para el uso de los equipos portátiles que se prestan para reuniones, conferencias y eventos similares.

4.5.6 UBICACIÓN Y PROTECCIÓN DE EQUIPOS DENTRO Y FUERA DE LAS INSTALACIONES

Los equipos de cómputo, dispositivos de telecomunicaciones y en especial, servidores y equipos de infraestructura tecnológica crítica serán ubicados en lugares seguros al interior de las instalaciones de la entidad, protegidos del polvo, temperaturas extremas, caída de objetos; igualmente alejados de puertas, ductos o ventanas con acceso desde el exterior. En caso de que se presenten condiciones que afecten la seguridad o protección contra amenazas ambientales para los equipos, la situación debe ser reportada por el colaborador a quien se la ha asignado su gestión.
Los equipos de cómputo de propiedad de MINJUSTICIA deben contar con la autorización del jefe de la dependencia a cargo, así como del Grupo de Gestión Administrativa para su retiro fuera de las instalaciones de la entidad, y tanto estos equipos como los propios de los colaboradores o terceros, que sean utilizados para gestionar la información de MINJUSTICIA deben ser adecuadamente protegidos de la siguiente manera:
* No se deben dejar desatendidos los equipos en lugares públicos.
* Se debe evitar exposición a campos electromagnéticos intensos.
* Se deben evitar golpes, transporte de equipos encendidos, robo o deterioro físico.
* Para el teletrabajo o trabajo remoto, las condiciones del lugar de trabajo deben permitir el cuidado de los equipos para evitar su daño, afectación o acceso no controlado por menores de edad o personas ajenas a la entidad.

4.5.7 MEDIOS DE ALMACENAMIENTO

El uso de medios removibles como USB o discos duros externos, así como copias a correos electrónicos públicos debe evitarse y es responsabilidad de los usuarios la información que sea manejada en estos no se debe realizar extracción o retiro de los activos de información originales que deban ser custodiados en la Entidad (sean análogos, digitales o electrónicos).

Los custodios delegados de los activos deben gestionar el respaldo de la información clasificada o reservada, de manera que se mantenga una o varias copias de los activos análogos, digitales y electrónicos cuya disponibilidad sea crítica, preferiblemente en medios separados y/o diferentes ubicaciones, con el fin de reducir los riesgos de daño o pérdida de información. La Subdirección

de Tecnologías y Sistemas de Información aplica los controles requeridos para la información, digital y electrónica, de acuerdo con las políticas, mejores prácticas, análisis de riesgos, con base en los recursos disponibles y en la gestión de los custodios.
La Subdirección de Tecnologías y Sistemas de Información tiene a cargo el contrato de transporte y custodia de las copias de respaldo de información (Backups) con un proveedor de este tipo de servicio, para el almacenamiento de las bases de datos de la Entidad. El proveedor del servicio de transporte y custodia debe cumplir con los requisitos de protección contra daño físico de los medios transportados, de manera que se conserven apropiadamente, se aíslen de factores ambientales como calor, humedad o campos electromagnéticos y se garantice que terceros no autorizados no puedan tener acceso a dichos medios. Así mismo, se deben cumplir con los lineamientos de continuidad, con el objetivo de velar por la disponibilidad de la información almacenada.

4.5.8 SERVICIOS PÚBLICOS DE APOYO

Las instalaciones de procesamiento de información, en especial el centro de datos, deben estar protegidas contra cortes de energía a través de UPS, y contar con un suministro alterno a través de planta eléctrica durante los posibles cortes que se puedan generar. En cuanto a los servicios de conectividad, serán gestionados por parte de la STSI, con base en los recursos asignados, canales alternos de respaldo, en caso de pérdida de disponibilidad.

4.5.9 SEGURIDAD DEL CABLEADO

El cableado eléctrico y de telecomunicaciones que transmite datos o sirve de soporte a los servicios de información de estar protegido frente a daños físicos, interceptación, interferencias o deterioro. El Grupo de Gestión Administrativa de la entidad deberá velar por la instalación subterránea de líneas de energía y telecomunicaciones, en la medida de lo posible, de forma separada para evitar interferencias.
Para el cableado de instalaciones críticas como el centro de datos se debe propender por la instalación de conductos blindados y cajas cerradas en los puntos de inspección y terminación, apantallamiento electromagnético, barreras técnicas y realización de inspecciones físicas periódicas para detectar conexiones al cableado no autorizadas. Se mantendrá acceso controlado a los patch panel y centros de cableado.

4.5.10 MANTENIMIENTO DE EQUIPOS

Los planes y contratos de mantenimiento de la infraestructura física estarán a cargo del Grupo de Gestión Administrativa o quien haga sus veces. En cuanto a los planes y contratos de mantenimiento preventivo de los equipos de cómputo y telecomunicaciones, los mismos estarán a cargo de la STSI, de manera que se asegure la disponibilidad e integridad permanente del hardware.

Los mantenimientos se deben programar, realizar y verificar con la frecuencia recomendada por el proveedor, de acuerdo con la fecha de adquisición y la antigüedad de cada equipo por parte de personal capacitado y autorizado para su ejecución, conservando los registros de cada uno de los mantenimientos realizados, sean éstos preventivos o correctivos. Es importante la inspección y aceptación por parte del usuario responsable del equipo, antes de recibirlo a satisfacción, una vez realizado el mantenimiento. La información contenida en el equipo no debe ser de carácter confidencial y las actividades de mantenimiento deberán ser supervisadas por el colaborador delegado por parte de la STSI.

4.5.11 DISPOSICIÓN FINAL O REUTILIZACIÓN SEGURA DE EQUIPOS

La STSI debe asegurar la implementación de los controles necesarios para la reutilización o desecho seguro de los equipos de hardware u otros soportes de almacenamiento que se vayan a trasferir a terceros, sea por donación, venta u obsolescencia tecnológica.
Toda la información de la entidad, en especial si es clasificada o reservada, incluyendo software que se encuentre instalado, será borrada de manera segura de los medios a desechar o donar, de manera que ésta no pueda ser recuperada por personas no autorizadas. Para implementarlo, las dependencias deben realizar una solicitud a la Mesa de Ayuda de TI, antes de obtener la autorización de parte del Grupo de Gestión Administrativa para la disposición de los medios. Desde la STSI se emitirá el diagnóstico técnico para el proceso correspondiente de bajas de equipos, y de igual forma se realizará la copia de la información, la cual se entregará al usuario (incluyendo imagen donde se informa el número de archivos y carpetas existentes; tanto antes, como después de realizada la copia). Posteriormente se ejecutará el borrado seguro en el equipo que se dará de baja. En caso de que el dispositivo se encuentre dañado y contenga información o software confidencial, debe ser destruido físicamente antes de desecharlo, para evitar que terceros puedan tener acceso a la misma.

4.6 CONTROLES TECNOLÓGICOS

4.6.1 DISPOSITIVOS DE USUARIO

La STSI implementa y gestiona los controles de seguridad perimetral de la red y se considera custodio de los equipos de hardware asignados a los usuarios de propiedad de MINJUSTICIA; en cuanto a la configuración, instalación de software licenciado y autorizado, monitoreo de software antivirus y antimalware; así como el mantenimiento preventivo y correctivo de equipos y software utilitario y de ofimática que se brinda a través de la Mesa de Ayuda de TI. Sin embargo, el uso seguro de cada equipo de usuario y el almacenamiento de información de la entidad en los repositorios dispuestos para ello, es responsabilidad del colaborador o tercero que lo tenga asignado en el inventario de bienes de la entidad.
En caso de contar con dispositivo móvil asignado por la entidad, se dará soporte y mantenimiento al mismo. Sin embargo, el uso de los móviles, sean estos de la entidad o de propiedad de cada colaborador, debe realizarse evitando el acceso a las aplicaciones e información clasificada o reservada de MINJUSTICIA, se prohíbe descargar estos activos en los equipos móviles y se recomienda adquirir e instalar un software antivirus o antimalware; así como evitar su pérdida o robo, en cuyo caso se debe reportar como un evento de seguridad a la Mesa de Ayuda de TI, para evaluar el riesgo, en caso de que se tuviera información confidencial de la entidad configurada o descargada. Se podrá requerir, eventualmente, del uso del dispositivo móvil, sea institucional o personal, para la implementación de controles de múltiple factor de autenticación para el acceso a plataformas y sistemas de la entidad.
En el caso que los contratistas y proveedores ingresen a las instalaciones del MJD sus equipos personales para el desarrollo de sus tareas y/o funciones, estos equipos personales deben pasar por la revisión y verificación de la mesa de ayuda de TI antes de permitir el acceso o conexión a la red de la entidad, estos equipos deben ser inspeccionados para asegurar que cumplan con las políticas de seguridad establecidas y como mínimo se exige que los equipos cuenten con software actualizado, medidas de protección como antivirus y cifrado de datos (si dicho cifrado de datos aplica), y se prohíbe el uso de dispositivos no autorizados para la transmisión o almacenamiento de información sensible. Tanto contratistas como proveedores deben conectarse a las redes

seguras de la entidad, garantizando que cualquier acceso a los sistemas esté supervisado y registrado, minimizando así el riesgo de fuga o compromisos de seguridad. Adicionalmente, se monitorea el acceso a la información y los datos a los que tienen permiso de interactuar, asegurando que solo accedan a la información necesaria para cumplir con sus tareas.

4.6.2 GESTIÓN Y RESTRICCIÓN DE ACCESOS

La asignación de los derechos de acceso privilegiado a las plataformas y demás recursos tecnológicos para su administración y monitoreo, se realiza por parte de la DTGIJ y STSI, de acuerdo con las responsabilidades y funciones de los colaboradores. Otros derechos de acceso privilegiado requeridos se regirán por el control de accesos especificado en la sección 4.3.5. de este documento.
La STSI a través de la administración de los recursos bajo su gestión, aplicará las restricciones para el acceso definidas por los propietarios de los activos a la información a las plataformas de red, correo, repositorios y sistemas de información e implementará, de acuerdo con los recursos disponibles, herramientas de Múltiple Factor de Autenticación, en especial para cuentas con accesos privilegiados como por ejemplo a programas utilitarios o acceso a información clasificada o reservada, así como de gestión de identidades digitales para los usuarios que acceden a los recursos informáticos, con el fin de garantizar que solamente las personas autorizadas tengan acceso a los recursos tecnológicos requeridos, es decir sistemas de información, recursos de hardware tales como servidores, redes y dispositivos de almacenamiento.
Solamente tendrán acceso al código fuente de las aplicaciones los colaboradores o terceros que lo requieran, con la respectiva autorización de la Dirección y Subdirección de Tecnologías y del propietario del software como activo de información, manteniendo por parte del grupo de sistemas de información el control de la integridad de las versiones en producción, pruebas y desarrollo.

4.6.3 GESTIÓN DE LA CAPACIDAD Y LA CONFIGURACIÓN

La STSI debe velar por la capacidad de procesamiento requerida en los recursos tecnológicos de la información de la entidad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica cuando sea necesario, mínimo una vez al año.
La STSI debe realizar las tareas de optimización de servicios tecnológicos y sistemas de información, al igual que la verificación de capacidad de los servicios de red de la entidad, así como la escalabilidad de los servicios de nube.
La STSI debe mantener y administrar la información documentada referente a las configuraciones de hardware, software, servicios y redes bajo su gestión, incluyendo la configuración de seguridad, de manera que sea posible su monitoreo y revisión periódica. Adicionalmente, se realizará depuración de la información almacenada en dispositivos o sistemas de información, en caso de no requerirse, contando con la autorización del propietario del activo y cumpliendo con los tiempos de retención determinados por las directrices de archivo, cuando aplique.

4.6.4 PROTECCIÓN CONTRA MALWARE

MINJUSTICIA proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, implementará las estrategias de comunicación y sensibilización necesarias para generar cultura de seguridad entre los colaboradores frente a los ataques de software malicioso.
La STSI debe contar con herramientas licenciadas tales como antivirus, antimalware, antispam y antispyware con actualización periódica de las últimas bases de datos de firmas del proveedor de servicios, las cuales reduzcan el riesgo de contagio de software malicioso y respalden la información contenida y administrada en la plataforma tecnológica de MINJUSTICIA y los servicios que se ejecutan en la misma. Los usuarios no están autorizados para realizar cambios en la configuración de los agentes de los mencionados sistemas, únicamente para realizar tareas de escaneo de medios.
La STSI debe velar por que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
Los usuarios de los servicios tecnológicos deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provengan de correos electrónicos desconocidos. Quienes sospechen o detecten alguna infección por software malicioso deben notificar de inmediato a STSI a través de la Mesa de Ayuda de TI, con el fin de ejercer los controles correspondientes.
El Responsable u Oficial de Seguridad de la Información, debe divulgar lineamientos para verificar la información relacionada con el software malicioso, y emitir comunicaciones de advertencia informativas.

4.6.5 GESTIÓN DE VULNERABILIDADES TÉCNICAS

El personal de infraestructura tecnológica, con la orientación del Responsable u Oficial de Seguridad de la Información, revisa periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica, por medio de la realización de pruebas de vulnerabilidades, con el objetivo de realizar la remediación viable sobre los hallazgos arrojados por dichas pruebas. Si se conocen nuevas vulnerabilidades

técnicas estas serán reportadas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición a la vulnerabilidad.
El Grupo de infraestructura tecnológica, con el apoyo del Oficial de Seguridad, debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas. Igualmente, generarán lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.
Por ningún motivo se pueden realizar análisis de vulnerabilidades o pruebas de intrusión, sin antes tener una autorización escrita emitida por la Dirección de Tecnologías y Gestión de la Información en Justicia. En caso contrario, el colaborador que incumpla, puede ser objeto de sanciones civiles, penales, económicas y sancionatorias de acuerdo a la ley y la normatividad vigente en la materia.

4.6.6 COPIAS DE SEGURIDAD DE LA INFORMACIÓN

La STSI debe gestionar y certificar la generación de las copias de respaldo y almacenamiento de la información crítica para la entidad, con base en los recursos disponibles y estableciendo los procesos y mecanismos para la realización de estas actividades. Los servicios de almacenamiento pueden ser en la nube o dentro de la infraestructura tecnológica propia.
MINJUSTICIA es responsable de velar porque los medios magnéticos que contienen la información sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con la seguridad física y medioambiental apropiada.
La STSI debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad. Se debe asegurar la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
La STSI debe llevar a cabo los procedimientos para realizar y documentar pruebas de recuperación periódicas a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario. Se deben definir las condiciones de transporte, transmisión o custodia de las copias de respaldo de la información que son almacenadas externamente. A través del procedimiento P-TI-04 de respaldo y restauración, se establecen las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la entidad.
Es responsabilidad de los propietarios de las aplicaciones o sistemas de información, solicitar a través de un caso a Mesa de Ayuda de TI la generación de copias de respaldo.
Los colaboradores de la entidad son responsables de hacer buen uso de los servicios tecnológicos del MINJUSTICIA, los cuales en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra colaboradores relacionados, legislación vigente y políticas y lineamientos de seguridad digital establecidas por la entidad.
Por ningún motivo se permite alojar en servidores información catalogada como personal, música, videos, etc. La única área que cuenta con autorización para guardar este tipo de archivo es la Oficina de Prensa y Comunicaciones, siempre y cuando correspondan con los activos de información gestionados por dicha dependencia.
Es responsabilidad de los colaboradores garantizar que la información de la entidad esté guardada en los repositorios dispuestos para tal fin. La STSI no es responsable de realizar copias de respaldo de equipos propios o institucionales asignados a usuarios finales por la entidad, únicamente se realizarán backups solicitados a través de un caso a Mesa de Ayuda de TI, siempre y cuando el usuario cuente con autorización del dueño o propietario de los activos de información a respaldar.
La STSI propenderá por la implementación de medidas de control y herramientas tecnológicas que permitan prevenir la fuga de datos de la entidad, a través del cifrado de información, restricciones a puertos USB para el uso de medios extraíbles, control de acceso, niveles de autorización, sensibilización de los colaboradores e idealmente, de acuerdo con los recursos asignados, una herramienta de prevención de pérdida de datos.

4.6.7 REGISTRO, SEGUIMIENTO Y MONITOREO

Los sistemas y plataformas deben contar con el registro de las actividades, excepciones, fallas y otros eventos relevantes, la STSI debe velar por su producción, almacenamiento, protección y análisis, en lo posible contando con herramientas y alertas automáticas que permitan realizar un monitoreo permanente del comportamiento anómalo de las redes, plataformas y sistemas de información, previniendo la ocurrencia de incidentes de seguridad de la información.

La STSI, en cabeza del Responsable u Oficial de Seguridad de la Información, el personal de los grupos de Infraestructura Tecnológica y de Sistemas de Información, debe definir las herramientas, responsable y periodicidad del monitoreo que se realizará a los registros de auditoría de los aplicativos donde operan los procesos misionales de la Entidad. Así mismo, deben reunirse para se deben analizar los resultados del monitoreo realizado.
La STSI en cabeza del personal de apoyo grupo de Sistemas de Información, debe velar por que los desarrolladores (internos y externos), generen registros (Log) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros. Se deberían incluir:
fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la STSI.

La STSI debe propender porque todos los sistemas de procesamiento de información, los equipos y demás servicios tecnológicos que lo ameriten se sincronicen con una única fuente de referencia de tiempo.

4.6.8 INSTALACIÓN DE SOFTWARE

Los usuarios tienen prohibido la instalación de software en los equipos del MINJUSTICIA, en caso de requerirlo, deben escalar la solicitud a la Mesa de Ayuda de la entidad, quien validará si es necesario con el Responsable u Oficial de Seguridad de la Información, si el software requerido está o no autorizado para su uso sin que represente un riesgo de seguridad digital. La STSI, en cabeza de la Mesa de Ayuda, debe mantener actualizada una lista del software autorizado dentro de la Entidad y realizar la correspondiente gestión de licencias, para dar cumplimiento a la normatividad sobre derechos de autor de software vigente.

4.6.9 SEGURIDAD DE REDES

SEGURIDAD DE LOS SERVICIOS DE RED

La STSI debe adoptar medidas para proteger la información mediante la gestión de disponibilidad de los recursos y servicios de red de MINJUSTICIA. Se implementan los controles necesarios para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

La STSI vela por la confidencialidad de la información, del direccionamiento y el enrutamiento de las redes de datos de MINJUSTICIA. Así mismo, se asegura que ningún equipo o dispositivo ajeno a la Entidad, pueda acceder a la red de MINJUSTICIA, sin previa autorización de la Subdirección, de jefe inmediato o supervisor de contrato, así como de la Mesa de Ayuda de TI, previa revisión del equipo de cómputo.
La STSI implementa las buenas prácticas de configuración establecidos por los fabricantes para los dispositivos de seguridad y de la red de la plataforma tecnológica de la Entidad. Se deben identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la entidad en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos no requeridos. Se implementan y administran las herramientas de aseguramiento del perímetro de la red, como el firewall, de manera que se monitoree y se restringa el tráfico de Internet.

USO DE SERVICIO DE INTERNET

La STSI debe administrar los recursos disponibles para la prestación del servicio de internet para las diferentes sedes de la entidad.
La STSI debe monitorear continuamente el canal o canales que prestan el servicio de internet, con el fin de prevenir y atender cualquier incidente que se presente tan pronto como sea posible. Se generan y monitorean
los registros de navegación y los accesos de los usuarios a Internet, los cuales pueden incluir tiempos de navegación y páginas visitadas por parte de los usuarios.
La STSI implementa controles de filtrado de contenido a través del proxy, de manera que se evite el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos; así como páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking o cualquier otro sitio web que vaya en contra de la ética, la moral, las leyes vigentes, salvo que sean requeridas para investigaciones científicas o por temas relacionados con la misión del Ministerio, con previa autorización de la DTGIJ y el Responsable u Oficial de Seguridad de la Información.
Los usuarios autorizados para hacer uso del servicio de internet son responsables de evitar prácticas o usos que puedan comprometer los servicios tecnológicos de la entidad o que afecten la seguridad de la información de MINJUSTICIA; deben hacer uso de este recurso en relación con las actividades laborales que así lo requieran, y según el perfil y roles autorizados por el jefe inmediato o supervisor del contrato, de acuerdo con los horarios establecidos y asignados.

SEGREGACIÓN DE REDES:

La STSI debe mantener las redes de datos segmentadas de acuerdo con un análisis de riesgos de cada una de las áreas y teniendo en cuenta el tipo de información y operaciones que ejecutan, por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Entidad.

La STSI debe instalar protección entre las redes internas de MINJUSTICIA y cualquier red externa, que esté fuera de la capacidad de control y administración de la Entidad. Se debe realizar de manera periódica el cambio de las claves de acceso a la red WIFI de la Entidad.

MENSAJERÍA ELECTRÓNICA Y OTRAS HERRAMIENTAS CORPORATIVAS

La STSI debe implementar controles que eviten el acceso no autorizado a los servicios de mensajería autorizados por la Entidad (correo institucional, proveedor de drive y otros repositorios institucionales, FTP autorizados) con el fin de evitar cualquier modificación o denegación del servicio.
La STSI debe velar por que los controles de autenticación desde redes públicas hacia los servicios de la entidad sean fuertes y en lo posible, contar con doble factor de autenticación.
El Ministerio asigna una cuenta de correo electrónico corporativo con dominio minjusticia.gov.co; la cual también posee una cuota con almacenamiento en nube. El titular de la cuenta de correo y/o a quien se asigne una cuenta institucional será el responsable de la información que se almacene en dicho recurso.
MINJUSTICIA a través de la STSI, define las pautas generales para asegurar un adecuado uso de la Suite de Proveedor (correo electrónico, grupos, nube, calendario, sitios y formularios) por parte de los usuarios. Se
deben generar y divulgar los lineamientos y directrices para el manejo adecuado de cuentas y grupos de correo electrónico; así como de las demás herramientas disponibles.
La STSI se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico, con el fin de evitar la propagación de software malicioso. Igualmente, implementa controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de mensajes.
El único servicio de correo electrónico controlado por MINJUSTICIA es el asignado directamente por la STSI, el cual cumple con todos los requerimientos técnicos y de seguridad para evitar

ataques informáticos, virus, spyware y cualquier otro tipo de software o código malicioso.
La cuenta de correo electrónico asignada es de carácter individual, por lo tanto, ningún colaborador debe compartirla o usar una cuenta que no sea la suya. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por MINJUSTICIA y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad. Los mensajes y la información contenida en el correo institucional deben estar relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo de MINJUSTICIA. El correo institucional no debe ser usado para asuntos personales. Los mensajes y la información contenida en los buzones de correo son propiedad del MINJUSTICIA y cada usuario, como responsable de su buzón, debe mantener únicamente los mensajes relacionados con el desarrollo de sus funciones.
Los usuarios de correo electrónico tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, amenazas o mensajes violentos, pornografía y demás contenidos que degraden la condición humana, atente contra la integridad de las personas o instituciones, resulten ofensivas. No es permitido el envío o recepción de archivos con extensiones ejecutables. Igualmente, está prohibido el reenvío automático o manual de correos institucionales con información clasificada o reservada a correos personales o de otras entidades, sin la correspondiente autorización del propietario de los activos de información. El servicio de correo electrónico debe ser usado de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos, sistemas de información e imagen de MINJUSTICIA.

Cuando un proceso, oficina, grupo o dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina de Comunicaciones de MINJUSTICIA o el medio formal autorizado para realizar dicha actividad.

El servicio de correo electrónico debe contar con respaldo de información de los buzones, este se realiza de manera periódica y segura.
El usuario debe evitar abrir, compartir, descargar archivos adjuntos o ingresar a enlaces en correos sospechosos. Siempre se debe confirmar con el emisor cualquier correo inesperado, aun cuando se trate de
un remitente conocido. No se debe dar información personal, de la entidad o financiera que se solicite en correos de dudosa procedencia. Es responsabilidad del usuario reportar un correo electrónico cuando crea que es sospechoso, a la STSI a través de la Mesa de Ayuda, con el fin de que el administrador tome las medidas necesarias para evitar su propagación dentro de la entidad.
Es responsabilidad de cada usuario asegurar el destino de la comunicación, si estas son listas de distribución, también debe revisarlas con el fin de evitar compartir información a personas no autorizadas. Está prohibido la creación, almacenamiento o intercambio de mensajes que atenten contra las leyes de derechos de autor.
Los buzones institucionales (como: contacto, atención al ciudadano, soporte técnico, control interno, etc.) deben tener un funcionario responsable, quien debe velar por su buen uso.

Es obligación del usuario realizar la activación de las respuestas automáticas en el servicio de correo de MINJUSTICIA cuando su ausencia sea mayor a tres (3) días; igualmente, ésta debe indicar quién es la persona asignada para cubrir su ausencia. Nota: La persona encargada de cubrir la ausencia debe estar autorizada por parte del jefe inmediato o supervisor del contrato.

USO REDES SOCIALES

La información que se publique por cualquier medio de internet, por parte de un colaborador de MINJUSTICIA, en redes sociales se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad, disponibilidad, daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en redes sociales que sea originada por la entidad debe ser autorizada por el líder de Comunicaciones y las áreas técnicas para ser socializadas de acuerdo con los objetivos estratégicos de la Entidad.
No se debe utilizar el nombre de la entidad en redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la institución. En caso de que los comentarios sean agresivos o con lenguaje no apropiado, el administrador de las redes sociales bloqueará o eliminará la cuenta que lo genere. No se permiten descargas o distribución de material obsceno, degradante, terrorista, abusivo o que calumnie a través de servicios sociales.
Para MINJUSTICIA, las administraciones de las cuentas de redes sociales están a cargo del proceso de la Oficina de Prensa y Comunicaciones de acuerdo con los procedimientos internos de la Entidad. El/La Jefe de la Oficina de Prensa y Comunicaciones tendrá la obligación de autorizar y validar las cuentas oficiales en redes sociales de MINJUSTICIA, en caso de encontrar una suplantación reportará el incidente de seguridad a través de la Mesa de Ayuda de la entidad.

4.6.10 USO DE LA CRIPTOGRAFÍA

Los colaboradores que manejen información confidencial al interior y/o exterior de la Entidad deben aplicar los controles criptográficos con las herramientas establecidas por la Dirección de Tecnologías y Gestión de la Información en reposo y en movimiento.
Todas las claves, usuarios con acceso a sistemas, datos y/o servicios de la Entidad, deben estar cifradas para la protección de la información.
Se debe cifrar la información de acuerdo con la criticidad de los activos de información, eligiendo la mejor opción:
• Cifrado completo del disco duro del equipo de cómputo.
• Cifrado por carpetas específicas.
• Cifrado de disco duro extraíble, USB u otros dispositivos de almacenamiento.
La STSI debe realizar valoraciones de riesgos para determinar el nivel de calidad del algoritmo de cifrado requerido. Deben estar establecidos los roles y responsabilidades para la implementación de las políticas y la gestión de llaves, donde haya segregación de funciones.
Se deben considerar las reglamentaciones o normas nacionales e internacionales, así como las buenas prácticas relacionadas a cifrado o protección de información. Se debe analizar el objetivo para el uso de los controles criptográficos (Confidencialidad, integridad, no repudio o autenticación).
Cuando se realiza intercambio de información el Ministerio de Justicia y del Derecho utiliza la plataforma de Xroad de interoperabilidad, de acuerdo con la Guía Despliegue Servidor de Seguridad Plataforma de Interoperabilidad del 2019 de MINTIC y al procedimiento para el intercambio de información. Xroad para el intercambio de datos utiliza protocolos criptográficos seguros a través HTTPS con TLS 1.2 y los mensajes cifrados aplicando el algoritmo RSA con la función Hash SHA512.
La STSI brinda soluciones de seguridad definidas para los componentes de autenticación y autorización con las firmas digitales.

4.6.11 CICLO DE VIDA DE DESARROLLO SEGURO

REQUISITOS Y PRUEBAS DE SEGURIDAD DE LAS APLICACIONES

La STSI velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos y lineamientos de desarrollo seguro adecuados para la protección de la información del MINJUSTICIA.

La STSI será la única dependencia de la Entidad con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a los requerimientos de las diferentes dependencias, con el fin de dar soporte, mantenimiento y seguridad de la información de los sistemas que operan en el MINJUSTICIA. En consecuencia, cualquier software que opere en la Entidad sin autorización y aval de la STSI, no será responsabilidad de esta, por lo tanto, no se le brinda soporte y no se le salvaguarda la información.
MINJUSTICIA asegura que el software adquirido y desarrollado por terceras partes, cumplirá con los requisitos de desarrollo seguro especificados en los estándares OWASP en su versión vigente, así como los principios de arquitectura para la ingeniería de sistemas seguros y codificación segura. Las áreas funcionales propietarias de sistemas de información en conjunto con la STSI incluirán requisitos de desarrollo seguro en la definición de requerimientos y, posteriormente se asegura que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.
Todos los sistemas de información o desarrollos de software deben tener un área funcional responsable de la administración y la STSI será el responsable de la custodia dentro de la Entidad. Las áreas funcionales responsables de la administración de los sistemas de información en acompañamiento con la STSI y el Responsable u Oficial de Seguridad de la Información deben establecer las especificaciones de adquisición o desarrollo de sistemas de información considerando siempre los requerimientos de seguridad de la información.
El área funcional responsable de la administración de los sistemas de información debe definir qué perfiles se deben configurar en los sistemas de información a desarrollar, igualmente, deben aprobar la asignación de estos perfiles cuando sea necesario.
La STSI debe entregar los ambientes de pruebas y producción libres de vulnerabilidades en sus sistemas operativos, y velar porque los proveedores de los servicios de desarrollo de sistemas información realicen y certifiquen pruebas de vulnerabilidades al producto de software entregado, éste debe contar con todas las vulnerabilidades remediadas. La STSI debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con los últimos parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema. Las áreas funcionales deben incluir los requisitos y cláusulas necesarias en los contratos con proveedores de software para garantizar la seguridad de las aplicaciones y la remediación de posibles vulnerabilidades que se detecten en cualquier etapa del ciclo de vida.
Los desarrolladores de software, sean internos o externos, deben cumplir con los siguientes requisitos:
• Construir los sistemas de información de tal manera que efectúen las validaciones de datos de entrada y la generación de datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
• Asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

• Suministrar opciones de desconexión o cierre de sesión de los sistemas de información (Logout) que permitan terminar completamente con la sesión o conexión asociada.
• Asegurar el manejo de operaciones sensibles o críticas de los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como token o el ingreso de parámetros adicionales de verificación.
• Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
• Velar porque no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
• Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción, así como prevenir la revelación estricta de directorios de los

sistemas de información construidos.
• Remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
• Evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales deben estar cifrados.
• Certificar el cierre de la conexión con las bases de datos desde los aplicativos tan pronto como éstas sean requeridas.
• Implementar controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en el repositorio destinado para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
• No realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.
• Proteger el código fuente de los aplicativos construidos, de tal forma que no pueda ser descargado ni modificado por usuarios no autorizados.
• Asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

La STSI debe propender porque cada vez que se pretenda implementar un sistema de información, este sea sometido a un análisis de vulnerabilidades supervisado por el responsable u Oficial de Seguridad de la Información, las cuales deben ser remediadas antes del despliegue en producción por las áreas encargadas.
Los datos utilizados para las pruebas funcionales, técnicas y de seguridad de los sistemas de información se deben seleccionar, proteger y gestionar adecuadamente, para evitar afectación de la información sensible de la entidad.
La STSI debe proteger los datos de prueba que se entregan a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción. Cada vez que se realicen copias de información de producción se debe contar con un registro que permita realizar la auditoría.
Cada vez que se requiera de una copia de información para ser utilizada en las pruebas, esta solicitud debe ser aprobada por el Subdirector de Tecnologías y Sistemas de información, el responsable u Oficial de Seguridad de la Información y del administrador de bases de datos.
Las pruebas de auditoría y otras actividades de evaluación independiente que abarquen la evaluación de los sistemas operativos o de información se deben planificar en conjunto entre el ente de control interno o externo, la DTGIJ y STSI.
La STSI debe velar porque todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas, soportadas, actualizadas y reconocidas en el mercado. Así mismo, exigirá la documentación técnica del producto de software, el código fuente (si aplica), la documentación requerida para uso y administración de los sistemas de información, sus repositorios y bases de datos, incluyendo manuales de usuario, a los proveedores externos. La STSI debe asegurar que los sistemas de información adquiridos y 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 STSI monitoreará, dirigirá y hará seguimiento a las actividades relacionadas con el desarrollo de software contratado con terceros, de acuerdo con los requisitos establecidos en la contratación, el compromiso de confidencialidad firmado y las obligaciones específicas de seguridad de la información de los proveedores.
En el desarrollo de software, la calidad del código es un factor clave para garantizar que los productos funcionen correctamente y satisfagan las necesidades de la Entidad. Uno de los principales indicadores de calidad es el coverage o cobertura de pruebas, que mide qué porcentaje del código ha sido ejecutado y verificado mediante pruebas automáticas. El proveedor

de desarrollo de software que aspire a entregar un producto confiable debe garantizar un nivel de cobertura mínimo del 85% antes de que el producto sea aceptado.
Este umbral de cobertura no es arbitrario, sino que refleja un estándar que equilibra la necesidad de eficiencia en las pruebas y la reducción de riesgos. Con una cobertura del 85%, se asegura que la gran mayoría del código ha sido probada, lo que aumenta la probabilidad de detectar errores, bugs o comportamientos inesperados antes de que el software llegue a producción. Una cobertura inferior a este porcentaje deja demasiadas áreas del código sin verificar, lo que podría resultar en la presencia de defectos en componentes críticos que no fueron probados adecuadamente.

SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN

La STSI debe proveer los recursos necesarios para la implementación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de pruebas y producción, la inexistencia de compiladores editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

El ambiente de pruebas se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo. El ambiente de producción debe utilizarse para la prestación de un servicio que involucra el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la entidad.
La STSI en cabeza del personal de apoyo de Sistemas de Información debe definir y documentar las reglas para la transferencia de software del ambiente de pruebas a producción y debe velar porque todo cambio que se deba realizar en los sistemas información en producción deba ser probados en un ambiente de pruebas antes de aplicarlos a los sistemas en producción, salvo que sean cambios de emergencia.
La STSI en cabeza del personal de Sistemas de Información debe propender porque los compiladores, editores y otras herramientas de desarrollo y utilitarios del sistema, no sean accedidos desde sistemas de producción cuando se no se requieren.
La STSI en cabeza del personal de apoyo de Sistemas de Información velará por que los usuarios usen diferentes perfiles para los ambientes de pruebas y producción, igualmente debe velar por que los menús desplieguen mensajes de identificación apropiados para reducir el riesgo de error.
Las áreas funcionales propietarias de los sistemas de información deben probar las migraciones entre los ambientes de pruebas y producción que han sido aprobadas. La STSI debe contar con un sistema de control de versiones para administrar los cambios en los sistemas de información de MINJUSTICIA.

GESTIÓN DEL CAMBIO

El responsable de gestionar un cambio de TI debe tener en cuenta el MSPI e identificar y registrar los cambios significativos. Se deben tener en cuenta los siguientes aspectos relevantes:

* Planificación y puesta a prueba de los cambios, valorar los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información.
* La aprobación formal para los cambios propuestos debe quedar con un soporte con las evidencias correspondientes.
* Verificar que no se compromete la disponibilidad, integridad y confidencialidad de la información.
* Comunicar todos los detalles de los cambios a todas las personas pertinentes.
* Se debe tener claro cuáles son las actividades para abortar cambios no exitosos y recuperarse de ellos, así como eventos no previstos.

* Contar con un suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.
* La STSI, con el responsable del cambio, debe velar por que se realice una adecuada planeación, pruebas, ejecución y documentación de los cambios a los servicios tecnológicos y/o sistemas de información de la Entidad.
* La STSI, en cabeza del Responsable u Oficial de Seguridad de la Información, debe velar por la valoración de los impactos potenciales en la ejecución de cambios a los servicios tecnológicos y/o sistemas de información de la Entidad.
* La STSI y el solicitante del cambio debe documentar de manera apropiada el proceso de aprobación formal de los cambios a los servicios tecnológicos y sistemas de información de MINJUSTICIA.
* El Responsable u Oficial de Seguridad debe revisar que los cambios propuestos a los servicios tecnológicos de la Entidad cumplan con los requisitos de seguridad digital.
* La STSI, con el apoyo de la Mesa de Ayuda, debe informar a la entidad la fecha y servicios que no estarán disponibles.
* La STSI, en cabeza del personal de apoyo para la Gestión de Cambios, debe verificarlos en caso de presentarse un incidente que lo requiera.

La STSI debe atender el P-TI-06 Procedimiento de control de cambios y desarrollo de software, para el manejo de los cambios en el software, aplicativos y sistemas de información del MINJUSTICIA.

5. FORMATOS Y REGISTROS UTILIZADOS

https://sig.minjusticia.gov.co/

CLASE	TÍTULO DEL DOCUMENTO	
NA	NA	

6. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
1	N.A
2	Como resultado de la revisión anual de la política de seguridad de la información, se actualizaron los lineamientos de algunos dominios, el alcance, los objetivos, roles y responsabilidades, en el marco de la mejora continua del sistema de gestión de seguridad de la información. Se crean los 4 acuerdos de confidencialidad relacionados en el punto 5 (Formatos y registros utilizados).

3	Como resultado de la revisión anual de la política de seguridad de la información, se modifica lo siguiente: • Se define cada uno de los términos del glosario. • Modificación a la sección: “EQUIPO DEL PROYECTO DE SEGURIDAD DE LA INFORMACIÓN”: Se incluye la Subdirección de Gestión de Información en Justicia. • Se modifica el título “Terminación de vinculación, vacaciones, licencias o terminación de contratos”. • Se adecúa el item “4.3 POLITICA DE SEGURIDAD EN LOS RECURSOS”. • Se modifica el numeral “4.5 LA POLITICA DE GESTIÓN DE ACCESO”, anexando lineamientos para el almacenamiento y debido tratamiento de la información laboral. Se anexa ítem para realizar backup, a los equipos dados de baja. Se incluye la política de definición de requerimientos de seguridad para proveedores, en el numeral “4.11 POLÍTICA PARA LA GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES”.
4	Como resultado de la revisión anual de la política de seguridad de la información, se modifica lo siguiente: • Se actualizó la política general de seguridad de la información de MJD y los objetivos, para simplificarlos. • Se reorganizaron todas las políticas específicas de acuerdo con el Anexo A de la Norma ISO 27001:2022. Se complementaron y actualizaron la mayoría de políticas, simplificando aspectos de redacción. • Se incluyeron políticas específicas para: segregación de funciones, seguridad para servicios de nube, seguridad de la información y relación con los proveedores, otras políticas organizacionales, teletrabajo y trabajo remoto y controles físicos. • Se dieron de baja los siguientes formatos de acuerdos de confidencialidad anteriormente relacionados con la Política de Seguridad, los cuales se incorporaron en los procesos correspondientes, de ingreso de personal y contratación: Acuerdo de Confidencialidad para funcionarios F-IC-G14-01 Acuerdo de Confidencialidad para Contratistas F-IC-G14-02 Acuerdo de Confidencialidad Proveedores F-IC-G14-03 Acuerdo de Confidencialidad con Convenio F-IC-G14-04

5	Como resultado de la revisión anual de la Política de Seguridad de la Información se lleva a cabo la actualización de la política en el marco de la mejora continua del sistema de gestión de seguridad de la información en cuanto a: * Para la gestión de activos el propietario o responsable de la información de cada una de las dependencias debe velar por que se lleve a cabo la validación y seguimiento del cumplimiento de los controles de seguridad definidos en la matriz de riesgos. * La protección de registros de datos personales se definió que Las áreas propietarias son las encargadas de asegurar que el tratamiento de estos datos cumpla con las normativas vigentes. Esto incluye la correcta clasificación, manejo y protección de los datos según las leyes y regulaciones aplicables. * Con respecto al uso de los dispositivos por parte de los contratistas y proveedores se definió que los contratistas y proveedores que ingresen a las instalaciones del MJD sus equipos personales para el desarrollo de sus tareas y/o funciones, estos equipos personales deben pasar por la revisión y verificación de la mesa de ayuda de TI. * En el ítem “Requisitos y pruebas de seguridad de las aplicaciones’’, se definió que el proveedor de desarrollo de software debe entregar a la entidad como mínimo una cobertura del 85% de aceptabilidad de aceptabilidad en cuanto a la seguridad de este.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma:	Firma:	Firma:
Nombre: Jair Caicedo Cortez	Nombre: José Eliberto Fonseca Ruiz	Nombre: Julio Cesar Rivera Morato
Cargo: Oficial de Seguridad de la Información	Cargo: Subdirector de Tecnologías y Sistemas de Información	Cargo: Director de Tecnologías y Gestión de información en Justicia