MINISTERIO DE TRABAJO
Y SEGURIDAD SOCIAL

DIRECCIÓN GENERAL ADMINISTRATIVA FINANCIERA

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL

DGAF-18.5-PO-01

Versión 4.0
San José, Costa Rica

Junio 2020

B. Tabla de aprobadores y revisores

Lista de Aprobadores y Revisores		
Rol	**Nombre/Cargo/Dependencia**	**Firma Digital**
Elaboró	MSc. Leda Hernández Cordero Coordinadora Unidad de Seguridad Informática Gestión de Calidad y Riesgo Departamento de Tecnologías de Información y Comunicación	LEDA ISABEL HERNANDEZ CORDERO (FIRMA) Firmado digitalmente por LEDA ISABEL HERNANDEZ CORDERO (FIRMA) Fecha: 2020.06.10 09:07:17 -06'00'
Revisó	MBA, MSc. Selena Aguilar Morales Unidad de Seguridad Informática Gestión de Calidad y Riesgo Departamento de Tecnologías de Información y Comunicación	SELENA AGUILAR MORALES (FIRMA) Firmado digitalmente por SELENA AGUILAR MORALES (FIRMA) Fecha: 2020.06.11 14:54:05 -06'00'
	MSc. Alexander Pineda Cordero Coordinador Unidad de Bases de Datos Departamento de Tecnologías de Información y Comunicación	ALEXANDER PINEDA CORDERO (FIRMA) Firmado digitalmente por ALEXANDER PINEDA CORDERO (FIRMA) Fecha: 2020.06.12 15:47:39 -06'00'
	Lic. Gilberth González Torres Coordinador Unidad de Proyectos y Gestión Administrativa Departamento de Tecnologías de Información y Comunicación	MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL Firmado digitalmente por GILBERT GONZALEZ TORRES (FIRMA) Fecha: 2020.06.12 13:53:57 -06'00'
	Lic. Julio Zamora Valerio Coordinador Unidad de sistemas de Información Departamento de Tecnologías de Información y Comunicación	JULIO CESAR ZAMORA VALERIO (FIRMA) Firmado digitalmente por JULIO CESAR ZAMORA VALERIO (FIRMA) Fecha: 2020.06.12 13:26:27 -06'00'
	Lic. Michael Vargas López Coordinador Unidad de Infraestructura Telecomunicaciones y Soporte Técnico Departamento de Tecnologías de Información y Comunicación	MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL Firmado digitalmente por MICHAEL ROBERTO VARGAS LOPEZ (FIRMA) Fecha: 2020.06.15 09:33:24 -06'00'

Aprobó	Lic. Jorge Víquez López Jefe Departamento de Tecnologías de Información y Comunicación Coordinador Comisión Institucional de Tecnologías de Información	JORGE VIQUEZ LOPEZ (FIRMA) Firmado digitalmente por JORGE VIQUEZ LOPEZ (FIRMA) Fecha: 2020.06.15 09:43:38 -06'00'
Autorizó	MSc. Geannina Dinarte Romero Ministra Ministerio de Trabajo y seguridad Social	CARMEN GEANNINA DINARTE ROMERO (FIRMA) Firmado digitalmente por CARMEN GEANNINA DINARTE ROMERO (FIRMA) Fecha: 2020.06.26 09:57:08 -06'00'

C. Índice

D. Antecedentes

Los avances en las tecnologías de información y comunicación, han convertido los activos de información del Ministerio de Trabajo y Seguridad Social en una de las herramientas más utilizadas en las labores diarias de este. Lo anterior justifica el diseño e implementación de medidas pertinentes para su protección contemplando los riesgos y amenazas a los que están expuestos.

La información es un activo esencial de la organización y requiere en consecuencia una gestión adecuada. Esto es especialmente importante en ambientes de trabajo cada vez más interconectados por medio de diversos mecanismos tecnológicos. Como resultado de esta creciente interconectividad, la información se expone a una variedad más amplia de riesgos, amenazas y vulnerabilidades asociadas a dichos riesgos, relevantes para la Institución.

Se utilizan dos marcos normativos de referencia para la Gestión de la Seguridad de la Información:

- La familia de normas INTE/ISO/IEC 27000, específicamente
    - Norma INTE/ISO/IEC 27000:2018 Técnicas de Seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario.
    - Norma INTE/ISO/IEC 27001:2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.
    - Norma INTE/ISO/IEC 27002:2016 Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para controles de seguridad de la información.
- Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de la República de Costa Rica, aprobadas mediante Resolución del Despacho de la Contraloría General de la República, Nro. R-CO-26-2007 del 7 de junio, 2007. Publicada en La Gaceta Nro.119 del 21 de junio, 2007.

Con base en el marco normativo en mención, es necesario que la Institución disponga de un Sistema de Gestión de Seguridad de la Información (SGSI) para administrar eficientemente el acceso a los activos de información.

La gestión de seguridad de la información es la herramienta para la protección de la información y tiene como objetivo asegurar la continuidad del Ministerio, minimizar los daños, maximizar el retorno de las inversiones, así como las oportunidades de la Institución frente a una amplia gama de riesgos y amenazas asociadas, que se logra implementando un conjunto adecuado de controles, incluyendo políticas específicas, procesos, procedimientos, estructuras organizativas. Estos controles deben ser establecidos, puestos en funcionamiento, supervisados, revisados y mejorados continuamente para asegurar el cumplimiento de los objetivos específicos de la seguridad de la información de la Institución. Esto debe hacerse en forma conjunta con otros procesos de la administración del Ministerio.

Además, la Gestión de la Seguridad de la Información debe estar alineada con los objetivos establecidos en el Plan Estratégico Institucional vigente (2018-2022) el cual establece las siguientes prioridades:

- Promover el cumplimiento efectivo y aplicación de las normas internacionales del trabajo, de la legislación laboral nacional y de las diferentes normativas sobre seguridad social.

- Desarrollar políticas activas que favorezcan el acceso al empleo decente, priorizando los grupos más afectados por la exclusión laboral, la informalidad y la pobreza.

- Servicios de calidad a nivel nacional basados en los principios de equidad, eficiencia, efectividad y oportunidad.

- Fortalecer la comunicación y el diálogo social entre los actores del mercado de trabajo, para que coadyuven a mejorar la calidad del empleo.

E. Presentación de la Política de Seguridad de la Información

1. Generalidades

Una Política de Seguridad de la Información es una forma de comunicarse con los funcionarios de la Institución, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos del MTSS.

Una Política de Seguridad de la Información es una descripción de lo que deseamos proteger y él por qué de esta protección y está orientada a que los funcionarios de la Institución y partes interesadas reconozcan la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de trabajo del MTSS.

Por lo tanto, las políticas de seguridad de la información establecen una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios para la gestión de la información.

2. Contenido

La Política General de Seguridad de la Información del Ministerio de Trabajo y Seguridad Social agrupa los siguientes aspectos:

- Declaración de la Política.
- Principios.
- Contenido.
- Objetivos.
- Alcance.
- Gobernanza.
- Revisión de la Política.
- Roles y Responsabilidades.
- Ámbitos de la Seguridad de la Información.
- Control Normativo.
- Divulgación y Promoción de la Política
- No cumplimiento y sanciones.

3. Declaración de la Política General de Seguridad de la Información

El Ministerio de Trabajo y Seguridad Social reconoce la importancia de los activos de información como pilar fundamental para el correcto funcionamiento y desarrollo de los procesos institucionales.

Estos activos están expuestos a riesgos, cuya materialización podría impactar en forma negativa la atención a los usuarios, por ello, es prioritario para la Administración Superior gestionar en forma adecuada la seguridad de la información con el objetivo de minimizar la exposición a estos riesgos.

Para lograr este objetivo, el Ministerio de Trabajo y Seguridad Social implementa un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma INTE/ISO/IEC 27000:2018 y su familia normativa, en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información N-2-2007-CO-DFOE de la Contraloría General de la República, así como las mejores prácticas internacionales, con el fin de proteger los activos de información Institucional.

El Ministerio de Trabajo y Seguridad Social establece esta Política con la cual se compromete a salvaguardar la Seguridad de la Información en el contexto del marco estratégico de la Institución. Para ello, la Institución deberá:

- Impulsar y fortalecer activamente los principios y objetivos de la Seguridad de la Información.
- Proveer los recursos necesarios para la implementación de esta política.
- Divulgar la Política de Seguridad de la Información en toda la organización y partes interesadas.
- Desarrollar y ejecutar un plan de mejora continua con el fin de asegurar una adecuada gestión de la seguridad de la información

Es responsabilidad de todas las dependencias de la Institución dar cumplimiento a esta Política.

4. Principios

La información debe ser protegida adecuadamente sin importar la forma que tome o los medios por los que se comparta, guarde o respalde, ya sea impresa, almacenada digitalmente, transmitida por correo o por medios electrónicos, proyectada o comunicada verbalmente. Por ello, se debe considerar los siguientes principios de seguridad:

- Integridad de la información:
  Mantener con exactitud la información tal y como fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- Confidencialidad:
  Asegurar el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización. Impedir la divulgación de información a otras personas, entidades o procesos no autorizados.

- Disponibilidad:
  Dar acceso a la información y a los sistemas a las personas autorizadas en el momento que así lo requieran.

- Mejora Continua:
  Implementar acciones dirigidas a obtener la mayor calidad posible de servicios de la Institución, dirigidos a mejorar continuamente los procesos de la Institución.

- No repudio
  Capacidad de probar la ocurrencia de un evento o acción realizado y sus entidades de origen

- Autenticidad
  Capacidad de probar la ocurrencia de un evento o acción realizado y sus entidades de origen

- Rendición de cuentas
  Dar trazabilidad fehaciente a la información mediante bitácoras de acceso

- Confiabilidad
  Capacidad de probar la ocurrencia de un evento o acción realizado y sus entidades de origen

5. Objetivos de la Política General

5.1 Objetivo General

Preservar las características de confiabilidad, integridad, confidencialidad, disponibilidad y cumplimiento de la información que utiliza, con el fin de respaldar sus procesos de misión crítica, como medio para asegurar la continuidad de las operaciones.

5.2 Objetivos Específicos

- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los usuarios internos de las tecnologías de información y Comunicación y de los servicios que estos prestan a la ciudadanía en general.
- Fortalecer la cultura de seguridad de la información en los funcionarios y terceros.
- Establecer la obligatoriedad del cumplimiento de las Políticas Específicas de Seguridad de la Información asociadas con la presente política, para lo cual cada Dependencia debe establecer los controles necesarios para su acatamiento.
- Procurar la continuidad del negocio frente a incidentes y eventos importantes.
- Minimizar el riesgo en los procesos más importantes y críticos de la Institución.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

6. Alcance

Esta política es de implementación y acatamiento obligatorio para todas las personas funcionarias de la Institución, Unidades Ejecutoras, Contratistas y personas externas que utilicen tecnologías y/o servicios provistos por el Ministerio de Trabajo y Seguridad Social, para lo cual deben cumplir lo establecido en las políticas específicas asociadas a esta Política General.

7. Gobernanza de la Seguridad de la Información

La gobernanza del Sistema de Gestión de la Seguridad de la información está establecida de la siguiente forma:

Plano funcional (Rol)	Área
Estratégico	Despacho del Jerarca Institucional
	Comisión Institucional de Tecnologías de Información
Ejecutor	Departamento de Tecnologías de Información y Comunicación.
Normativo	Dirección de Asuntos Jurídicos

8. Revisión de la Política General y Políticas Específicas

La Política General y las Políticas Específicas deben ser revisadas con una frecuencia mínima bianual y podrían ser actualizadas cada vez que se realicen cambios relevantes en la Institución que afecten la adecuada protección de la información, considerando dentro de estos: cambios en la misión, objetivos estratégicos, productos estratégicos, infraestructura, marco normativo, personal y/o procedimientos relacionados con la protección de la información.

Los cambios deben ser revisados por el Departamento de Tecnologías de Información y Comunicación, la Dirección de Asuntos Jurídicos, posteriormente

aprobados por la Comisión Institucional de Tecnologías de Información y en última instancia, por el Despacho del Jerarca Institucional.

9. Roles y Responsabilidades

Tareas	DJI	CITI	DTIC	DMTSS	DAJ	PI	DGIRH	EGSI
Oficializar la Política General de Seguridad de la Información	R/A	I	I/C	I				
Oficializar las Políticas Específicas de Seguridad de la Información	R/A	I	I/C	I				
Apoyar al equipo de gestión de la seguridad de la información	R	I	I	I	I		I	I/C
Promover la actualización oportuna de la Política General de Seguridad de la Información	R/A	I	R/A					I/C
Facilitar los espacios necesarios para la divulgación oportuna en la organización y partes interesadas	R/A	R/A	R					
Incluir responsabilidades en función de Seguridad de la Información en el Manual Descriptivo de Cargos los funcionarios y en el Reglamento Autónomo del Ministerio de Trabajo y Seguridad Social	R	I	C	R			R	I/C
Revisar la Política General y Políticas Específicas.		R/A	R/A		C			C
Aprobar la Política General y Políticas Específicas.	R/A	I	R					R
Denunciar cualquier incumplimiento a la política general y a las políticas específicas asociadas a esta.		I	R	R				
Realizar revisiones aleatorias sin previo aviso en cualquier área de la Institución sobre el cumplimiento de la política general y las políticas específicas ligadas a esta y reportar los hallazgos al Equipo de Gestión de Seguridad de la Información para la aplicación de las medidas correctivas pertinentes.		I	R					
Proponer mejoras o ajustes a la Política General o Políticas específicas producto del conocimiento técnico especializado en la materia.			I					R
Acatar lo establecido en las políticas de seguridad de la información implementando los controles necesarios para este fin.	R	R	R	R	R	R	R	R
Divulgación y promoción las políticas de seguridad de la información	R/A	I	I/C	I		I	I	I/C
R: Responsable | A: Rinde cuentas | C: Consultado | I: Informado								

DJI	Despacho del Jerarca Institucional
CITI	Comisión Institucional Tecnologías Información
DTIC	Departamento de Tecnologías de Información y Comunicación
DMTSS	Dependencias del Ministerio de Trabajo y Seguridad Social
DAJ	Dirección de Asuntos Jurídicos
PI	Partes Interesadas (externas)
DGIRH	Departamento de Gestión Institucional de Recurso Humano
EGSI	Equipo de Gestión de Seguridad de la Información

10. Marco de referencia de la Seguridad de la Información

La Política de Seguridad de la Información, toma como marco de referencia los criterios de la Norma INTE/ISO/IEC 27001:2018 así como los controles establecidos

en la Norma INTE/ISO/IEC 27002:2016. (Anexo 1 Políticas Específicas de Seguridad de la Información).

Nombre del Documento	Código	Disposición
Norma INTE/ISO/IEC 27000:2018 Técnicas de Seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario y su respectiva familia.	Norma INTE/ISO/IEC 27000:2018 Norma INTE/ISO/IEC 27001.2014 Norma INTE/ISO/IEC 27002.2016	Con el uso de la familia de normas del SGSI las organizaciones pueden desarrollar un marco de referencia para la gestión de la seguridad de sus activos de información. **Localización**

11. Control Normativo

Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de la República, Aprobadas mediante Resolución del Despacho de la Contralora General de la República, Nro. R-CO-26-2007 del 7 de junio, 2007.

Nombre del Documento	Código	Disposición
Reglamento Autónomo de Servicio del Ministerio de Trabajo y Seguridad Social.	Decreto No. 27969-TSS y sus reformas. del 23 de junio de 1999.	Establece las normas para regular las condiciones de servicio bajo las cuales han de desempeñar sus funciones, tareas y labores los servidores del Ministerio de Trabajo y Seguridad Social; por lo cual debe modificarse el reglamento autónomo de servicios existente. **Localización**
Normas Técnicas para la gestión y el control de las	N-2-2007-CO-DFOE del 7 de junio del 2007.	Toda Institución Pública debe establecer un Marco de control y procurar una mejor

tecnologías de información, citada.		gestión de dichas tecnologías por parte de las organizaciones de conformidad con lo establecido en la Ley General de Control Interno Nro. 8292 del 31 de julio del 2002. **Localización**
Plan Estratégico Institucional	PEI-2018-2022.	Herramienta estratégica de mayor relevancia para la gestión institucional; en el que están definidos los principales criterios que permitirán a la institución desarrollar el liderazgo que le corresponde cumplir, como ente rector del Sector Trabajo. **Localización**
Protección de la Persona frente al tratamiento de sus datos personales	Ley N° 8968 07 de julo del 2011.	Marco legal que tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. **Localización**

12. Divulgación y Promoción de la Política

La Administración Superior es la responsable de divulgar y promover de forma continua las políticas, estándares y procedimientos de seguridad de la información en el MTSS, con el fin de sensibilizar y concienciar tanto a funcionarios como a terceros sobre este tema.

13. No cumplimiento y Sanciones

Las faltas y las eventuales sanciones asociadas con su incumplimiento, serán establecidas institucionalmente por las instancias competentes, según lo establece el Reglamento Autónomo de Servicio del Ministerio de Trabajo y Seguridad Social, ya que el Reglamento que se menciona ya fue citado.

F. Glosario

Nombre/Siglas	Definición
Activo	Aquello que tiene valor para la organización. Hay muchos tipos de activos, incluyendo: información, software, hardware, servicios, personas e intangibles.
Amenaza	Causa potencial de un incidente no deseado, que puede ocasionar daños a un sistema u organización. (INTE/ISO/IEC 27000:2018).
CDs (Compact Disc-Read Only Memory) - DVD (Digital Versatile Disc Read Only Memory)	Son dispositivos de almacenamiento, discos ópticos, que emplean una luz láser en lugar de un imán para leer y escribir bits de datos en una capa reflectante. Los datos en un disco óptico están grabados formando una espiral. Para representar unos y ceros lo que se hace es perforar la superficie usando un láser de una determinada frecuencia La diferencia de capacidad existente entre CD, DVD y discos Blue-Ray se debe simplemente el tamaño de estas marcas, las cuales dependen de la frecuencia y tamaño del rayo láser, cuanto menor sean, más datos se pueden representar en la misma superficie y el resultado es un disco de más capacidad. (Rebollo Pedruelo, Miguel, Dispositivos de Almacenamiento, Universidad Politécnica de valencia).
Confidencialidad	Propiedad de que la información no esté disponible o divulgada a individuos, entidades o procesos no autorizados. (INTE/ISO/IEC 27000:2018).
Continuidad del Negocio	Procesos Capacidad de la organización para continuar suministrando productos o servicios a niveles predefinidos aceptables, posterior a un incidente disruptivo. (INTE/ISO 22301:2015).
Control/Controles	Medida que modifica un riesgo. (INTE/ISO/IEC 27000:2018).

Disponibilidad	Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada. (INTE/ISO/IEC 27000:2018).
DTIC	Departamento de Tecnologías de Información y Comunicación.
Gobernanza de Seguridad de la Información	Sistema por el cual son dirigidas y controladas las actividades de seguridad de la información de una organización. (INTE/ISO/IEC 27000:2018).
Hardware	Todos los componentes electrónicos, eléctricos y mecánicos que integran una computadora o cualquier dispositivo informático.
Integridad	Propiedad de exactitud y completitud. (INTE/ISO/IEC 27000:2018).
Log-on	Se conoce de esta forma a los protocolos establecidos en la norma ISO 27001 para establecer controles de inicio de sesión seguros. Dentro de los cuales destacan: Corroboración de la identidad del usuario, muestra advertencias ante un intento de ingreso fallido, del cual deberá mantenerse un registro y darlo a conocer a los responsables. Un manejo apropiado de las sesiones inactivas, así como también establecer límites en el acceso. (INTE/ISO 27002:2016).
MTSS	Ministerio de Trabajo y Seguridad Social.
Objetivo	Resultado por alcanzar
Organización	Persona o grupo de personas con roles y responsabilidades, propias, autoridades y relaciones para alcanzar sus objetivos. (INTE/ISO 22301:2015).
PEI	Plan Estratégico Institucional.
PETIC	Plan Estratégico de Tecnologías de Información y Comunicación.

Política	Intenciones y dirección de una organización expresada formalmente por la Alta Dirección. (INTE/ISO/IEC 27000:2018).
Riesgo	Resultado de la incertidumbre sobre los objetivos. (INTE/ISO/IEC 27000:2018).
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, rendición de cuentas, no repudio y confiabilidad. (INTE/ISO/IEC 27000:2018).
SGSI	Sistema de Gestión de Seguridad de la Información.
Software	Programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.
TI	Tecnologías de Información
Trazabilidad	Capacidad para seguir el histórico, la aplicación o la localización de un objeto (ISO 9000:2015)
USB (Universal Serial Bus)	Es un dispositivo de almacenamiento que utiliza una memoria flash para guardar información. Memorias USB (Universal Serial Bus) Son dispositivos de almacenamiento que utilizan memoria tipo flash (memoria no volátil y programable, similar a las EEPROM - memoria ROM que puede ser programada, borrada y reprogramada eléctricamente) para guardar información y no necesita pilas. Es una unidad pequeña, liviana, extraíble y re escribible. Estas memorias se han convertido en el sistema de almacenamiento y transporte personal de datos más utilizado, desplazando en este uso a los tradicionales disquetes, y a los CD. Se pueden encontrar en el mercado memorias de 1, 2, 4, 8, 16, 32, 64 y hasta 128 GB. Esto supone, como mínimo, el equivalente a 180 CD de 700 MB. (Boletín Naturalis Facultad de Ingeniería Universidad Autónoma de México. Ing. Francisco Miguel Pérez

	Ramírez fcom1216@yahoo.com.mx Profesor de Carrera en la División de Ciencias Básicas de la Facultad de Ingeniería de la UNAM.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

G. Control de Cambios o Versiones

Control de Cambios y Versiones				
Versión Modificada	**Fecha de Revisión**	**Motivo de la Actualización**	**Elaboró**	**Firma**
3.0	29/4/2020	Cuarta actualización de las Políticas de Seguridad de la Información	MSc. Leda Hernández Cordero. Coordinadora Seguridad Informática Gestión de Calidad y Riesgo	

H. Anexos

Cuadro de Anexos					
N° Anexo	**Dirección**	**Departamento**	**Código o Número del Documento Anexado**	**Nombre del Anexo**	**Página donde se ubica el anexo**
1	DGAF	DTIC	__	Anexo 1 Políticas específicas	20

Anexo 1

Políticas Específicas de Seguridad de la Información

Las Políticas Específicas de Seguridad de la Información descritas en este Anexo, toman como marco de referencia los criterios de las Normas INTE/ISO/IEC 27000:2018, INTE/ISO/IEC 27001:2014 y los objetivos de control y controles de la Norma INTE/ISO/IEC 27002:2016.

A. Descripción

N° Artículo	Nombre	Descripción
Capítulo 1. Organización de la Seguridad de la Información		
Organización interna		
1.	Directrices para la gestión del riesgo en la seguridad de información.	El DTIC debe desarrollar un plan de gestión del riesgo de Seguridad de la Información en el cual se deben establecer las directrices para el manejo del riesgo involucrado. La Administración Superior comunicará este plan a quienes considere necesario.
2.	Segregación de funciones	El MTSS debe velar porque ninguna persona pueda acceder, modificar o utilizar activos de información sin autorización o detección. Las actividades que incluyan acceso a dichos activos deben ser realizadas por una persona y supervisadas por otra persona.
3.	Contacto con autoridades	El MTSS debe identificar las autoridades pertinentes a las que pueda acudir en el caso de que un incidente de seguridad de la información lo amerite. Además, tener procedimientos vigentes que especifiquen cuándo y por medio de quiénes las autoridades (de cumplimiento de leyes, organismos de reglamentación y autoridades de supervisión) deben contactarse, y cómo los incidentes de seguridad de la información identificados deben reportarse de

		manera oportuna (por ejemplo, si se sospecha que se está incumpliendo la ley).
4.	Contacto con grupos de Interés	El DTIC debe mantener contacto con grupos de interés especial en materia de seguridad de la información, así como con asociaciones de profesionales, a fin de mejorar el conocimiento sobre las mejores prácticas y mantenerse al día con la información relevante sobre seguridad de la información. Se debe promover la participación en foros sobre temas de Seguridad de la Información para mantener actualizado su conocimiento y ser apoyo estratégico al MTSS.
5.	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe integrarse en la metodología de gestión de proyectos de la Institución, con el fin de asegurar que los riesgos de seguridad de la información sean identificados y tratados como parte de un proyecto.
1.2 Dispositivos móviles y teletrabajo		
6.	Control de dispositivos móviles	Deben adoptarse en el Ministerio controles de seguridad para gestionar los riesgos que se presentan por el uso de dispositivos móviles (computadoras portátiles, memorias USB, discos externos provistos por el Ministerio), de manera que no se vea comprometida la operación de los dispositivos y la información de la Institución.
7.	Teletrabajo	La Administración debe elaborar modelos contractuales que establezcan los mecanismos de control y gestión del teletrabajo considerando en ellos la disminución de los riesgos en la seguridad de la Información. Dichos modelos deberán suscribirse entre la persona funcionaria y la jefatura inmediata.
Capítulo 2 Seguridad ligada a los recursos humanos		
2.1 Previo al empleo		
8.	Investigación	El Departamento de Gestión Institucional de Recursos Humanos debe verificar los

		antecedentes de todos los candidatos al empleo de acuerdo con las leyes, regulaciones y normas éticas vigentes en la Institución y en el país. Así como realizar todas las verificaciones necesarias para confirmar la autenticidad de la información suministrada por el candidato a ocupar un cargo antes de su contratación definitiva.
9.	Condiciones del empleo	Los funcionarios y contratistas, como parte de su obligación contractual con la Institución, deben aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones del Ministerio en cuanto a la seguridad de información.
2.2 Durante el empleo		
10.	Responsabilidades del Jerarca del Ministerio	Es responsabilidad del Jerarca de la Institución comunicar a los funcionarios la obligatoriedad del cumplimiento de las políticas y procedimientos de seguridad de la información.
11.	Concientización y educación en seguridad de la información	La Administración Superior debe asegurar que los funcionarios de la Institución, y cuando sea necesario los contratistas, sean concientizados y reciban formación y actualización en el tema de seguridad de la información
12.	Proceso disciplinario	Las faltas y las eventuales sanciones asociadas con el incumplimiento a estas políticas de seguridad de la información, serán establecidas institucionalmente por las instancias competentes, según lo establece el Reglamento Autónomo de Servicio del Ministerio de Trabajo y Seguridad Social.
Capítulo 3 Gestión de activos		
3.1 Responsabilidad por los activos		
13.	Inventario de activos	Los activos asociados con la información y los recursos para el procesamiento de esta deben ser identificados y se debe elaborar y mantener un inventario de esos activos.

14.	Identificación del propietario de los activos	Los activos relacionados con la información registrada en el inventario, deben tener un propietario, el cual deberá ser responsable de la gestión apropiada de este durante todo el ciclo de vida del activo.
15.	Uso aceptable de los activos	Es responsabilidad de los funcionarios administrar, mantener y cuidar la seguridad de los activos de información (Hardware, Software, equipos auxiliares, instalaciones entre otros) para las labores específicas de su puesto en la Institución y no se permite el uso para labores distintas. No está autorizada la instalación, actualización o reemplazo de hardware o software de su estación de trabajo, a menos que se tenga una autorización.
16.	Devolución de activos	Al término de su relación laboral, contrato o acuerdo, el funcionario o usuario externo, debe hacer la devolución de los activos siguiendo el procedimiento establecido para ello. De igual forma se debe actuar en caso de requerir un cambio del mismo.
3.2 Clasificación de la información		
17.	Clasificación de la información	El dueño de la información debe clasificarla en términos de su valor, criticidad, requisitos legales y sensibilidad a la divulgación o a la modificación no autorizada.
18.	Etiquetado de la información	La información debe ser etiquetada de acuerdo al esquema de clasificación de la misma adoptado por la Institución.
19.	Manejo de los activos	Se debe desarrollar e implementar controles para el manejo de los activos de acuerdo con el esquema de clasificación de la información adoptado por la organización.
3.3 Manejo de los medios de almacenamiento		
20.	Gestión de medios removibles	EL DTIC debe implementar controles para gestionar la seguridad de la información cuando se utilicen dispositivos removibles (cintas, discos

		duros removibles, CDs, DVDs y unidades externas USB, entre otros) de manera que no se comprometa la información de la Institución contenida en dichos medios, así como los dispositivos físicos de almacenamiento. Solamente deben utilizarse medios extraíbles bajo autorización expresa del DTIC.
21.	Eliminación de medios	EL DTIC debe establecer mecanismos formales para la eliminación segura tanto de los medios de almacenamiento como de la información contenida en ellos, a fin de minimizar el riesgo de pérdida o fuga de información confidencial El DTIC deberá contar con la autorización expresa del funcionario que tiene asignado el medio de almacenamiento antes de proceder con la disposición (eliminación) del medio y de la información contenida.
22.	Traslado de medios físicos	Los medios de almacenamiento que contienen información sensible deben ser protegidos durante su transporte de un punto de origen a un punto de destino contra el acceso no autorizado, mal uso o corrupción. Para ello, el DTIC deberá contar con mecanismos para controlar y mantener registro de personas autorizadas para entregar, transportar y recibir los medios de almacenamiento conteniendo datos sensibles.
Capítulo 4 Control de Acceso de los Usuarios		
4.1 Requisitos de la Institución para el control de acceso de los Usuarios		
23.	Política de control de acceso	El Ministerio debe establecer y documentar una política de control de acceso de los usuarios basada en la seguridad de la información y los requisitos Institucionales. Esta política deberá ser revisada en forma periódica con una frecuencia mínima anual.
24.	Acceso a las redes y a los servicios de red	Los funcionarios deben tener acceso únicamente a las redes y servicios de red autorizados y que estén relacionados con las labores que realizan.
4.2 Gestión de cuentas de usuario		

25.	Registro y cancelación de usuarios	EL DTIC debe implementar un mecanismo formal para la activación o inactivación (registro y cancelación) de cuentas de usuarios para la asignación de derechos de acceso a la red, servicios de red y sistemas informáticos. El Director o Jefe responsable de la información debe solicitar en forma escrita al DTIC la creación, suspensión, modificación y revocación de los privilegios sobre el uso de los activos de información de su competencia y particularmente de los usuarios de su área, basándose en los principios de necesidad de conocer.
26.	Gestión de derechos de acceso privilegiados	Se debe restringir y controlar la asignación y el uso de derechos de acceso privilegiados.
27.	Gestión de la información secreta de autenticación de usuarios	La asignación de información secreta de autenticación debe ser controlada a través de un proceso formal de gestión. Los usuarios deberán mantener la información de autenticación personal secreta en todo momento.
28.	Revisión de los derechos de acceso de los usuarios	Los propietarios o administradores de los activos de información deben revisar con intervalos regulares, al menos una vez al año los derechos otorgados a los usuarios de la red y diferentes sistemas de información de la Institución con el fin de asegurar que los accesos correspondan a los estrictamente necesarios para el ejercicio de sus funciones. La Administración Superior en coordinación con el DTIC tienen la potestad, de suspender en cualquier momento los accesos a los activos de información, en caso de comprobarse mal uso de estos privilegios.
29.	Eliminación o ajuste de los derechos de acceso	Los derechos de acceso de los funcionarios y usuarios externos a la información y a los recursos para procesarla, deben ser eliminados al finalizar la relación laboral con la Institución, contrato de trabajo o deberían ser modificados

		cada vez que se realicen cambios en el perfil del puesto.
4.3 Responsabilidades de los usuarios		
30.	Uso de la información secreta de autenticación	Los usuarios deben seguir las políticas de la Institución en el uso de la información secreta de autenticación, asegurando que no se divulgue a otras partes, incluidos los jerarcas del Ministerio
4.4 Control de acceso a sistemas y aplicaciones		
31.	Restricción de acceso a la información	El acceso a la información debe estar restringido y basarse en los requisitos de los perfiles de acceso de cada funcionario en los respectivos sistemas y aplicaciones.
32.	Procedimientos de accesos (*log-on*) seguros	Donde sea requerido por la política de control de acceso, se debería controlar el acceso a los sistemas y a las aplicaciones por medio de un procedimiento de acceso (*log-on*) seguro.
33.	Administración de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurarse de la calidad de las contraseñas.
34.	Uso de programas utilitarios privilegiados	El DTIC debe controlar y restringir estrictamente el uso de programas utilitarios para evitar que sobrepasen los controles de los sistemas y aplicaciones.
35.	Control de acceso al código fuente de programas	DTIC debe restringir el acceso al código fuente, manuales y documentación correspondientes a los sistemas en producción, además, debe definir los mecanismos para actualizar la información en caso de que se realicen modificaciones a esos sistemas. Solamente los funcionarios autorizados podrán tener acceso a esta información.
Capítulo 5 Criptografía		
5.1 Controles de criptografía		

36.	Política sobre el uso de controles criptográficos	El DTIC debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
37.	Gestión de llaves	El DTIC debe desarrollar e implementar un procedimiento sobre el uso, protección y el tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
Capítulo 6 Seguridad física y ambiental		
6.1 Áreas seguras		
38.	Perímetro de seguridad física	La Administración Superior y los funcionarios deben garantizar que todos los activos de información y los recursos de procesamiento de la misma se encuentren dentro de un perímetro de seguridad física consistente con los riesgos que podrían sufrir. Las áreas de acceso restringido deben estar claramente identificadas para proteger el acceso no autorizado.
39.	Controles de acceso físico	La Administración Superior en coordinación con el DTIC, debe definir e implementar controles relacionados con la administración, las condiciones de ambiente y el acceso físico al DTIC y a la Sala de Servidores (espacio destinado para ubicar los equipos de comunicaciones de la red institucional) o cualquier espacio del Ministerio que tenga equipos de comunicación y de almacenamiento (repositorio de datos). Es responsabilidad del DTIC mantener un registro de las personas que ingresan o visitan las áreas de acceso restringido, con el fin de proteger los activos que ahí se encuentran. Las Oficinas Regionales que cuentan con cuartos de comunicaciones o gabinetes para administración de enlaces de red, también deben contar con estos mecanismos de control.

40.	Seguridad de oficinas, despachos e instalaciones	Se debe contar con un mecanismo de control que permita la gestión de las áreas de acceso restringido. Se debe considerar 1) Las instalaciones de acceso restringido deben estar ubicadas de manera que eviten el acceso al público. 2) Las áreas de acceso restringido deben permanecer cerradas bajo llave o con dispositivo de control. 3) Se debe evitar dejar sin atención las oficinas ubicadas en áreas restringidas en horas laborales.
41.	Protección contra amenazas externas y ambientales	La Institución debe asesorarse y tomar medidas para que el equipo informático, medios de respaldo, cableado eléctrico y de telecomunicaciones que dan soporte a la operativa del Ministerio de Trabajo se encuentren protegidos contra amenazas externas y ambientales tales como, incendio, pérdidas altas o bajas de voltaje, humedad o calor extrema, filtraciones en las cañerías u otras fuentes de aguas internas, disturbios civiles y todas aquellas que por su naturaleza puedan afectar el equipo.
42.	Cambios en espacio físico	Las Dependencias del Ministerio que necesiten realizar cambios (creación, distribución de oficinas/personal, instalación o desinstalación de equipo, impresoras o cualquier otro recurso informático provisto por el Ministerio) deben solicitar al DTIC un estudio de factibilidad técnica y el visto bueno a este, con el fin de no afectar la infraestructura tanto física como tecnológica. Es responsabilidad del DTIC realizar un análisis de viabilidad de cambios solicitados por las Dependencias, que afecten las labores que el funcionario ejecuta con ese equipo; estos cambios son: movimiento de computadoras, creación de nuevas oficinas, instalación o desinstalación de equipo (Hardware), creación de nuevos punto de red entre otros.
43.	Trabajando en áreas seguras	Todo funcionario, proveedor de servicios o persona ajena al MTSS que ingresen al DTIC deben ser acompañados por un funcionario de

		este, con el fin de supervisar su visita o su trabajo y evitar daños a la infraestructura o datos. Las áreas seguras desocupadas, deben estar físicamente cerradas y periódicamente revisadas. La Administración Superior debe asegurarse de que la empresa de Seguridad contratada por la Institución designe funcionarios para realizar una revisión obligatoria de bolsos, maletines y computadoras portátiles, (donde esté presente el servicio contratado) con el fin de detectar salidas de equipo no autorizadas.
44.	Áreas de acceso público y de entrega y carga	Se debe controlar los puntos de acceso tales como áreas de entrega y carga así como otros puntos por donde podrían entrar personas no autorizadas a las instalaciones y si es posible, aislarlos de los recursos de procesamiento de la información para evitar accesos no autorizados.
45.	Colocación y protección del equipo	El equipo de cómputo debe estar colocado y protegido de manera en que se evite el acceso no autorizado a la información y así reducir los riesgos de amenazas ambientales y peligros.
46.	Servicios de soporte	El equipo debería ser protegido contra fallas de energía u otras interrupciones causadas por fallas en los servicios de soporte
47.	Seguridad del Cableado	El cableado de energía y de telecomunicaciones que transporta datos o soporta servicios de información debe estar protegido de interceptación, interferencia o daño.
48.	Mantenimiento del equipo	La Administración Superior debe procurar que todo equipo custodiado por los funcionarios del Ministerio reciba periódicamente mantenimiento para asegurar su disponibilidad. El mantenimiento del equipo debe ser realizado únicamente por los funcionarios del DTIC o proveedores contratados por la Administración Superior.

49.	Remoción de activos	El equipo, la información o el software no deben ser llevados fuera del sitio sin autorización previa.
50.	Seguridad del equipo y los activos fuera de las instalaciones	El MTSS debe contar con las medidas de seguridad y controles para prevenir daño, hurto, pérdida de la confidencialidad, fidelidad y disponibilidad de la información en aquellos equipos que por razones laborales se encuentren fuera de las instalaciones de la Institución.
51.	Seguridad en la reutilización o eliminación de equipos	La unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del DTIC con la autorización del funcionario que tiene asignado el equipo debe revisar y validar todo equipo que contenga medios de almacenamiento para asegurarse que cualquier dato sensible o licenciado sea removido y que se sobrescriba de manera segura antes de desecharse o donarse. La eliminación de la información contenida en el equipo debe ser autorizada por escrito por el funcionario que tiene asignado el equipo y con el visto bueno de la Jefatura del mismo.
52.	Desecho (baja) de equipo de cómputo retiro de bienes	La Proveeduría Institucional debe realizar el desecho del equipo de cómputo y componentes al menos una vez al año, con el criterio técnico del DTIC, aplicando la normativa vigente de acuerdo con el Reglamento para el Registro y Control de Bienes de la Administración Central.
53.	Equipo desatendido por el usuario	Todo funcionario que requiera dejar equipo desatendido, o alejarse de su equipo debe terminar las sesiones activas y bloquear su computadora (CTRL +ALT+SUPR/DELETE) o la combinación de las teclas Windows y la letra “L”. El DTIC debe habilitar un mecanismo automático para bloqueo del equipo, por ejemplo, un protector de pantalla protegido con contraseña. Todo funcionario al finalizar su jornada laboral y en fines de semana, debe apagar la computadora, pantalla y todo equipo de oficina que no requiera estar activo.

54.	Política de “Escritorio limpio” y “Pantalla limpia”	Todos los funcionarios deben guardar los documentos sensitivos, computadoras portátiles, discos y medios magnéticos bajo llave. Toda la información tanto física como digital debe protegerse independientemente del lugar en el que se encuentre. Se debe borrar o destruir información delicada de pizarras, rotafolios o papelógrafos una vez finalizada una reunión. No se deben dejar llaves de escritorios u oficinas sin supervisión, cada funcionario es responsable de administrar las llaves originales y las copias que se le han encargado y debe guardarlas en un lugar seguro. Cuando están desatendidas las computadoras deben cerrarse las sesiones o protegerlas con un mecanismo de bloqueo de pantalla.
Capítulo 7 Seguridad de las operaciones		
7.1 Procedimientos y responsabilidades operacionales		
55.	Instructivos de operación documentados	Deben elaborarse instructivos para las actividades operacionales asociadas con los recursos de comunicaciones y de procesamiento de información, tales como arranque y apagado del computador, respaldo, mantenimiento de equipos, manejo de medios, gestión y seguridad de la sala de cómputo y la utilización de correo entre otros.
56.	Gestión de cambios	El DTIC debe implementar un control de cambios de la organización, en los procesos de negocio, recursos de procesamiento de la organización y en los sistemas que afecten la seguridad de la información. Además, es necesario establecer las responsabilidades y los procedimientos formales de gestión para asegurar el control satisfactorio de todos los cambios. Cuando se realizan los cambios, debe conservarse una

		bitácora de auditoría conteniendo toda la información pertinente.
57.	Gestión de la capacidad	El DTIC debe realizar en conjunto con la Administración Superior y en alineamiento con el PEI y PETIC, el plan de gestión de capacidad, considerando como insumo las mejoras a sistemas actuales, la capacidad de medios de almacenamiento, de recursos humanos, de redes de comunicación, con el fin de proyectar los requerimientos futuros de los servicios provistos por TI.
58.	Separación de ambientes de desarrollo, pruebas y operación.	El DTIC debe mantener por separado los ambientes de prueba, desarrollo, base de datos y producción de sistemas de información, con el fin de reducir el riesgo de acceso o cambios no autorizados. Deben existir controles de acceso a cada uno de los ambientes citados.
7.2 Protección contra código malicioso (malware).		
59.	Controles contra el código malicioso.	El DTIC debe implementar controles de detección, prevención y recuperación, con el fin de protegerse de código malicioso, acompañado de una adecuada toma de conciencia del usuario.
7.3 Respaldo		
60.	Respaldo de la información	Las copias de respaldo de la información, del software y de las imágenes del sistema, deben ser obtenidas y analizadas periódicamente de acuerdo con una política acordada de respaldo.
7.4 Registro y seguimiento		
61.	Registro de eventos	El DTIC debe generar, mantener y revisar periódicamente los registros de eventos de las actividades de los usuarios, las excepciones, las fallas y los eventos de seguridad de la información. Las bitácoras de eventos pueden contener datos confidenciales e información de identificación personal, de ser posible, los administradores de los sistemas no deben tener permiso para borrar

		o desactivar los registros de sus propias actividades.
62.	Protección del registro de información (log)	El DTIC debe implementar controles para proteger contra acceso y cambios no autorizados a la información de bitácoras y problemas con las facilidades de registro a las mismas.
63.	Registros del administrador y el operador	El DTIC debe contar con mecanismos de control que registren las actividades del administrador y el operador del sistema. Estos registros deben revisarse en forma periódica con una frecuencia mínima anual.
64.	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información relevantes dentro del Ministerio o dominio de seguridad se deben sincronizar con una sola fuente de tiempo de referencia.
7.5 Control de software operativo		
65.	Instalación de software en los sistemas en producción	El DTIC debe implementar controles para la instalación y cambios de software en los sistemas en operación ya sean estos desarrollados internamente o provistos por terceros.
7.6 Gestión de vulnerabilidades técnicas		
66.	Gestión de vulnerabilidades técnicas	El DTIC es responsable de revisar los avisos de vulnerabilidades emitidos por las organizaciones internacionales y realizar las recomendaciones que estimen necesarias para la correcta operación de los recursos tecnológicos a nivel institucional.
67.	Restricciones en la instalación de software	Ningún funcionario está autorizado a instalar, actualizar o reemplazar hardware o software de su estación de trabajo, a excepción de los funcionarios del DTIC o los autorizados para realizar dicha tarea. Todo hallazgo de software o hardware encontrado por la Auditoría o el DTIC que haya sido instalado o utilizado sin autorización en una estación de trabajo o servidor, debe ser notificado a la Dirección responsable y a la Administración Superior, para

		que se establezcan las medidas correspondientes. Cualquier instalación o reemplazo de hardware o software de una estación de trabajo o Servidor deben solicitarse a través de la herramienta definida por el DTIC para esto.
Capítulo 8 Seguridad de las comunicaciones		
8.1 Gestión de seguridad de la red		
68.	Controles de red	El DTIC debe establecer controles que prevengan accesos no autorizados a los recursos de la red, tanto por parte de funcionarios internos como de personas externas al MTSS. Cualquier equipo o periférico que se requiera conectar debe cumplir con los controles de seguridad establecidos con el fin de verificar el cumplimiento de los requisitos mínimos de seguridad que deben cumplir los equipos que se conecten a la red institucional.
69.	Seguridad de los servicios de red	Se deben identificar e incluir en los acuerdos de nivel de servicio de red, los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red, ya sean servicios provistos internamente o subcontratados.
70.	Segregación de redes	El DTIC debe separar la arquitectura de red en subredes de acuerdo a los distintos niveles de seguridad que se requieran y a la clase de información contenida en los sistemas que integran esas redes.
8.2 Transferencia de información		
71.	Intercambio de información	Se deben establecer políticas, procedimientos y controles formales para proteger la transferencia de información que se realice mediante el uso de todo tipo de recursos de comunicación.
72.	Acuerdos de transferencia de información	Se deben establecer acuerdos para la transferencia segura de información del negocio entre la Institución y partes externas.

73.	Mensajería electrónica	Se debe proteger apropiadamente la información involucrada en la mensajería electrónica.
74.	Acuerdos de confidencialidad o no divulgación	La Administración Superior debe establecer y mantener actualizados los requisitos de confidencialidad que se apeguen a las necesidades de la Institución, para la protección de la información. El funcionario del Ministerio debe firmar un acuerdo de confidencialidad comprometiéndose a cumplir la política de confidencialidad de la información y lo que ésta representa, cuando su superior jerárquico así lo considere. El Departamento de Gestión de Capital Humano será el responsable de confeccionar dicho acuerdo y velar porque los funcionarios de la Institución lo firmen.
Capítulo 9 Adquisición, desarrollo y mantenimiento de sistemas		
9.1 Requisitos de seguridad de sistemas de información		
75.	Especificación de requerimientos de seguridad	Los requisitos relacionados con la seguridad de la información deberían ser incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
76.	Asegurar los servicios de aplicaciones en las redes públicas	Se debe proteger la información involucrada en los servicios de aplicaciones que pasan a través de redes públicas de la actividad fraudulenta, de la disputa contractual y de la divulgación y modificación no autorizada.
77.	Protección de las transacciones de servicios de aplicación	Se debe proteger la información involucrada en las transacciones de servicios de aplicación para prevenir la transmisión incompleta, el mal enrutamiento y la alteración, la divulgación, la duplicación o la reproducción no autorizada del mensaje.
9.2 Seguridad en los procesos de desarrollo y soporte		
78.	Política de desarrollo seguro	El DTIC deberá contar con un procedimiento para desarrollo interno de sistemas que contemple los mecanismos de seguridad

		necesarios para reducir los riesgos durante el desarrollo de los sistemas.
79.	Control de cambios de software y sistemas de información	El DTIC debe implementar un procedimiento de control de cambios durante el ciclo de vida del desarrollo de sistemas que deberá estar contemplado en el procedimiento para desarrollo interno de sistemas.
80.	Revisión técnica de las aplicaciones después de realizar cambios de plataforma de operación	Las aplicaciones críticas de la Institución deben ser revisadas y probadas cuando se cambian las plataformas de operación, para asegurar que no hay impacto negativo en las operaciones del Ministerio o en la seguridad.
81.	Restricciones en los cambios a los paquetes de software	Las modificaciones a los paquetes de software deben limitarse a modificaciones necesarias y todos los cambios deben ser estrictamente controlados.
82.	Principios de ingeniería de sistemas seguros	Se deben establecer, documentar, mantener y aplicar principios de ingeniería de sistemas seguros a todos los esfuerzos de implementación de sistemas de información.
83.	Ambiente de desarrollo seguro	Se deben establecer y proteger adecuadamente los ambientes seguros para el desarrollo y la integración de sistemas que cubren todo el ciclo de vida de desarrollo del sistema, tomando en cuenta que un ambiente de desarrollo seguro incluye personas, procesos y tecnología asociados con el desarrollo y la integración de los sistemas.
84.	Supervisión del desarrollo de software contratado externamente.	La Administración Superior debe establecer una comisión contraparte, integrada por el propietario solicitante del software, personal del DTIC y de la Proveeduría Institucional, con el fin de garantizar que, al contratar el desarrollo de software por parte de terceros, se apliquen las metodologías para gestión de proyectos y desarrollo de sistemas establecidas por la Institución, para cumplir con los requisitos de

		seguridad y los requisitos del usuario dueño de la información. La empresa contratada para el desarrollo debe firmar un contrato confeccionado por la Proveeduría Institucional encargada de elaborar contratos, que asegure la propiedad del código fuente de los programas informáticos al MTSS, salvo excepciones según el tipo de contrato.
85.	Pruebas de seguridad de sistemas	El DTIC debe realizar y documentar pruebas de funcionalidad de la seguridad durante el desarrollo del sistema.
86.	Pruebas de aceptación del sistema	Se deben establecer programas de pruebas de aceptación y los criterios relacionados para los nuevos sistemas de información, las actualizaciones y las nuevas versiones.
9.3 Pruebas de datos		
87.	Protección de los datos de prueba	Los datos de prueba deben ser cuidadosamente seleccionados, protegidos y controlados.
Capítulo 10 Relaciones con los proveedores		
10.1 Seguridad de la información en la relación con los proveedores		
88.	Política de seguridad de la información para las relaciones con los proveedores	Se deben acordar y documentar los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización.
89.	Abordar la seguridad dentro de los acuerdos de proveedores	Se deben establecer y acordar los requisitos de seguridad de la información pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar componentes de infraestructura de TI para la información de la Institución.
90.	Adquisición de Hardware y Software	Los acuerdos con proveedores deben incluir los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de servicios y productos de tecnologías de información y comunicaciones. El DTIC en coordinación con la Proveeduría

		Institucional debe establecer y documentar los mecanismos y procedimientos de seguridad necesarios para que, al adquirir hardware o software (de sistema, de aplicación o de programación), se evalué la trayectoria del proveedor, la continuidad del producto y sus certificaciones. La seguridad debe ser considerada a lo largo de todo el proceso de adquisición, desde la especificación de los requerimientos hasta la implantación del software o la instalación del hardware. Cualquier adquisición de equipo informático o software se debe coordinar con el DTIC para asegurar el cumplimiento de las políticas de seguridad informática de la Institución. El proveedor debe firmar un acuerdo escrito de integridad, confeccionado por la Proveeduría Institucional en coordinación con el DTIC, en el que asegure que todas las características del hardware o software están documentadas y que no existen mecanismos ocultos que puedan comprometer la seguridad informática. El software de aplicación denominado “llave en mano” que se adquiera, no debe comprometer a la Institución a recurrir a la empresa proveedora cada vez que necesite alguna modificación, salvo casos muy específicos y autorizados por la Administración Superior.
10.2 Gestión de la entrega de servicios del proveedor		
91.	Seguimiento y revisión de los servicios de proveedores	Las Dependencias de la Institución, en conjunto con el DTIC deben dar seguimiento, revisar y auditar de forma periódica con una frecuencia mínima anual, la entrega de servicios de los proveedores de activos tecnológicos.
92.	Gestión de cambios en los servicios de proveedores	La Institución debe gestionar los cambios a la provisión de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de la información, procedimientos y controles, teniendo en cuenta la criticidad

		de la información del Ministerio, los sistemas y procesos implicados, y la revaluación de los riesgos.
Capítulo 11 Gestión de incidentes de seguridad de la información		
11.1 Gestión de incidentes y mejoras en la seguridad de la información		
93.	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para asegurarse de tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
94.	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información deben ser reportados a través de canales de gestión adecuados tan pronto como sea posible.
95.	Reporte de debilidades de seguridad de la información	Tanto los funcionarios del Ministerio como contratistas que utilizan los sistemas y servicios de información de la Institución deben reportar cualquier debilidad observada o sospechosa de la seguridad de la información en los sistemas o servicios.
96.	Evaluación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados y se debe decidir si serán clasificados como incidentes de seguridad de la información.
97.	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información se deben responder de acuerdo con los procedimientos documentados.
98.	Aprendiendo de los incidentes de seguridad de la información	La Institución debe utilizar el conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información para minimizar la posibilidad o el impacto de incidentes en el futuro.
99.	Recolección de evidencia	La Institución debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la información, que puede servir como evidencia. EL DTIC debe colaborar y apoyar ante un

		incidente que involucre causas legales a recopilar la información de forma íntegra.
Capítulo 12 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
12.1 Continuidad de la Seguridad de la Información		
100.	Planificación de la continuidad de la seguridad de la información	La Institución debe determinar sus requisitos de seguridad de la información y planificar la continuidad de la gestión de seguridad de la información en situaciones adversas, tales como una crisis o desastre.
101.	Implementación de la continuidad de seguridad de la información	La Institución debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa. Las Direcciones en conjunto con el área de DTIC deben desarrollar un proceso de Gestión de Continuidad de negocio para garantizar la capacidad necesaria para soportar su operativa.
102.	Verificar, revisar y evaluar la continuidad de seguridad de la información	La Institución debe verificar el establecimiento e implementación de los controles de continuidad de la información a intervalos regulares para asegurarse de que sean válidos y efectivos durante situaciones adversas.
12.2 Redundancias		
103.	Disponibilidad de recursos de procesamiento de información	Los recursos de procesamiento de la información deben ser implementados con redundancia suficiente para cumplir los requisitos de disponibilidad.
Capítulo 13 Cumplimiento		
13.1 Cumplimiento de los requisitos legales y contractuales		
104.	Identificación de la legislación aplicable y los requisitos contractuales	La Administración Superior y el DTIC deben tener identificada la legislación aplicable en su ámbito de competencia con el fin de definir e implementar los controles necesarios para la administración de los Recursos de Tecnología de Información.

105.	Derechos de propiedad intelectual	La Institución debe implementar procedimientos apropiados para asegurarse del cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario.
106.	Protección de registros	Se deben proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada, de conformidad con los requisitos legales, reglamentarios, contractuales y de negocio.
107.	Privacidad y protección de datos personales	Debe asegurarse la privacidad y la protección de los datos personales según lo dispuesto en la legislación y la reglamentación pertinente cuando sea aplicable.
108.	Regulación de los controles criptográficos	Se deben utilizar controles criptográficos en cumplimiento con todos los acuerdos, leyes, y regulaciones pertinentes.
13.2 Revisión de seguridad de la información		
109.	Revisiones independientes de seguridad de la información	El enfoque de la Institución para la gestión de seguridad de la información y su implementación (por ejemplo, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) deben ser revisados de forma independiente por un tercero contratado para este fin a intervalos planificados o cuando se produzcan cambios significativos.
110.	Cumplimiento con las políticas y normas de seguridad	Los administradores deben revisar periódicamente el cumplimiento del procesamiento de la información y procedimientos dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad
111.	Revisiones de cumplimiento técnico	Los sistemas de información deben ser revisados regularmente para el cumplimiento de las políticas y las normas de seguridad de la información de la organización.