

MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL

DIRECCIÓN GENERAL ADMINISTRATIVA FINANCIERA DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

POLÍTICAS DE SEGURIDAD INFORMÁTICA

DGA-DTIC-POL-001

Versión 3.0

Octubre 2015

HISTORIAL DE REVISIONES

Fecha	Versión	Descripción	Autor
06/01/2011	1.0	Revisión del documento original	DTI
10/01/2011 a 13/01/2011	1.1	Revisión de redacción y ortografía	Candy Retana
24/08/2011	1.2	Revisión del contenido y redacción	Gabriela Romero
11/10/2011	1.3	Revisión de la redacción del Documento por parte de la Dirección de Asuntos Jurídicos.	Ivannia Barrantes
12/10/2011	1.3	Revisión sobre contenido del documento	Edgar Cubero
18/03/2014	2	Revisión y alineación del documento original a ISO-27001-2005	Selena Aguilar Morales
02/04/2014	2	Revisión y validación de la versión 2	Leda Hernández Cordero
04/04/2014	2	Revisión y aprobación de la versión 2	Daniel Sáenz Hernández
26/08/2014	2.1	Revisión de la redacción del Documento por parte de la Dirección de Asuntos Jurídicos.	Viviana Mora Cerdas Patricia Steiner Batres Gerardo Bogantes Rivera
01/07/2015	2.1	Revisión de redacción del artículo 58 del documento en reunión del DTIC con la Oficialía Mayor	Rolando Chinchilla Masis Daniel Sáenz Hernández
22/07/2015	2.2	Revisión del Artículo 18 en reunión Dirección Asuntos Jurídicos-DTIC	Ivannia Barrantes Equipo DTIC
16/09/2015	2.3	Se eliminó el artículo 8 por recomendación de Asuntos Jurídicos, lo cual cambió la numeración de los artículos.	Daniel Sáenz Hernández
16/09/2015	2.3	Se modificaron los artículos 2,5,8,9,13,14,15,16,17,23,29,31,33,38,40,47,48,50,52,55,57,58,62,64,67,68,69,71,	Daniel Sáenz Hernández

		72,77,82 y 89 del actual documento	
14/10/2015	2.3	Dirección General y Oficialía Mayor modifica parcialmente los artículos 15, 19, 20 y 33	Rolando Chinchilla Masís
15/10/2015	3	Los cambios realizados hacen que se cambie la versión	Daniel Sáenz Hernández

HISTORIAL DE CAMBIOS

Fecha Aprobación	Versión	Descripción
10/01/2011	1.1	Se realizaron los cambios acordados el 06/01/2011 en reunión general del DTI
13/01/2010	1.1	Se realizaron las correcciones señaladas por Candy Retana en su revisión.
26/08/2011	1.2	Se realizaron las correcciones señaladas por la Directora Administrativa, Gabriela Romero.
11/10/2011	1.3	Se realizaron las correcciones señaladas por Ivannia Barrantes Subdirectora de Asuntos Jurídicos
13/10/2011	1.3	Se realizaron los cambios acordados con Edgar Cubero y se modificó el artículo 39 para dejar más claro lo referente a Teletrabajo. Se agregaron los artículos 41 y 61 referentes a bitácoras y logs.
18/03/2014	2	Se realizó el estudio del documento original para alinearlos con la Norma ISO-27001-2005. Resultado de este estudio se cambió la estructura del documento basado en los controles de la citada norma. Además para cumplir con esta estructura se eliminaron 30 artículos, se crearon 45, se quedaron igual aunque con diferente numeración 44 artículos y uno se mantuvo el nombre y cambió la redacción.

02/04/2014	2	Se revisó el documento producto de la alineación con la Norma ISO-27001-2005 y se validan los cambios realizados.
09/09/2014	2.1	Se realizaron los cambios sugeridos por la Dirección de Asuntos Jurídicos
15/01/2015	2.1	Se realizan modificaciones solicitadas por la Dirección General Administrativa Financiera
15/01/2015	2.1	Oficialía Mayor solicitó revisión por parte de Afumitra OM-0027-2015 del 15 de enero del 2015
21/01/2015	2.1	Afumitra manifiesta que no tiene observaciones sobre el documento Afumitra-SGA-0007-2015 del 21 de enero de 2015
29/01/2015	2.1	Oficialía Mayor remite al Despacho del Ministro con su visto bueno
02/07/2015 22/07/2015	2.2	Se cambia la redacción del artículo 58 del documento Se cambia el artículo 18, se le elimina el tercer párrafo.
14/10/2015	2.3	Se cambia la redacción de los artículos 15,19,20 y 33 por parte de la Oficialía Mayor
15/10/2015	3.0	Se cambia la versión a raíz de todos los cambios generados por la revisión del documento.
15/10/2015	3.0	Oficialía Mayor remite al Despacho del Ministro con su visto bueno


COMISION DE TRABAJO

El documento generado fue revisado por los funcionarios del DTIC

TABLA DE CONTENIDO

HISTORIAL DE CAMBIOS	3
COMISION DE TRABAJO	4
1 INTRODUCCIÓN.....	9
2 OBJETIVO	10
3 ALCANCE	10
4 CONSIDERACIONES GENERALES	10
5 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	12
6 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA	12
7 CONTENIDO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA	13
8 GLOSARIO.....	15
9 DESCRIPCIÓN DE LAS POLITICAS	22
CAPÍTULO I POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.....	22
ARTÍCULO 1. COMPROMISO DE LA ADMINISTRACIÓN CON LA SEGURIDAD DE LA INFORMACIÓN.....	22
ARTÍCULO 2. DOCUMENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	22
ARTÍCULO 3. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	22
ARTÍCULO 4. DIRECTRICES PARA LA GESTIÓN DEL RIESGO EN LA SEGURIDAD DE INFORMACIÓN	22
ARTÍCULO 5. SEGURIDAD INFORMÁTICA EN EL PLAN ANUAL OPERATIVO	22
ARTÍCULO 6. INCLUSIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PLAN ANUAL DEL MTSS	22
CAPÍTULO II ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	24
ARTÍCULO 7. DIVULGACIÓN Y PROMOCIÓN	24
ARTÍCULO 8. DEFINICIÓN DE LAS RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	24
ARTÍCULO 9. USO DE HERRAMIENTAS INFORMÁTICAS	24
ARTÍCULO 10. ACUERDOS DE CONFIDENCIALIDAD	24
ARTÍCULO 11. CONTACTOS CON GRUPOS DE INTERÉS	25
ARTÍCULO 12. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN Y CONTROLES DE AUDITORÍA PARA SISTEMAS DE INFORMACIÓN	25
ARTÍCULO 13. IDENTIFICACIÓN DE RIESGOS RELACIONADOS CON ENTIDADES EXTERNAS	25
ARTÍCULO 14. DIRIGIENDO LA SEGURIDAD AL REALIZAR ACUERDOS CON TERCEROS	25
CAPÍTULO III GESTIÓN DE ACTIVOS.....	26
ARTÍCULO 15. INVENTARIO DE ACTIVOS	26
ARTÍCULO 16. IDENTIFICACIÓN DEL PROPIETARIO Y CUSTODIO DE CADA TIPO DE INFORMACIÓN	26
ARTICULO 17. USO ACEPTABLE DE LOS ACTIVOS	26
ARTÍCULO 18. DIRECTRICES DE CLASIFICACIÓN, ETIQUETADO Y MANEJO DE INFORMACIÓN	27

ARTÍCULO 19. DEVOLUCIÓN DE ACTIVOS	27
ARTÍCULO 20. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	28
ARTÍCULO 21. AVISOS DE VULNERABILIDADES	28
ARTÍCULO 23. ACCESO A LOS ARCHIVOS Y DOCUMENTOS FÍSICOS	29
ARTÍCULO 24. CONTROLES DE ACCESO FÍSICO	29
ARTÍCULO 25. SEGURIDAD DE OFICINAS, DESPACHOS E INSTALACIONES	29
ARTÍCULO 26. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	29
ARTÍCULO 27. CAMBIOS EN ESPACIO FÍSICO	30
ARTÍCULO 28. TRABAJO EN ÁREAS SEGURAS	30
ARTÍCULO 29. ÁREAS DE ACCESO PÚBLICO	30
ARTÍCULO 30. MANTENIMIENTO DEL EQUIPO.....	30
ARTÍCULO 31. SEGURIDAD DEL EQUIPO FUERA DE SITIO	30
ARTÍCULO 32. SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE EQUIPOS.....	31
ARTÍCULO 33. DESECHO (BAJA) DE EQUIPO DE CÓMPUTO RETIRO DE BIENES	31
ARTÍCULO 35. ACTUALIZACIONES DE SEGURIDAD Y CAMBIOS	32
ARTÍCULO 36. SEGREGACIÓN DE FUNCIONES	32
ARTÍCULO 37. ACCESO AL AMBIENTE DE PRODUCCIÓN	32
ARTÍCULO 38. GESTIÓN DE LA CAPACIDAD	32
ARTÍCULO 39. PROTECCIÓN CONTRA CÓDIGO MALICIOSO	32
ARTÍCULO 40. RESPALDO (BACKUP)	33
ARTÍCULO 41. RESPALDO DE DOCUMENTOS CON FIRMA DIGITAL	33
ARTÍCULO 42. RETENCIÓN DE INFORMACIÓN	33
ARTÍCULO 43. ADMINISTRACIÓN DE CONTROLES DE ACCESO A LA RED	33
ARTÍCULO 44. IDENTIFICACIÓN DEL EQUIPO EN LA RED	33
ARTÍCULO 45 SEGMENTACIÓN DE REDES	34
ARTÍCULO 46. COMPUTACIÓN MÓVIL Y COMUNICACIONES	34
ARTÍCULO 47. INTERCAMBIO DE INFORMACIÓN	34
ARTÍCULO 48. MEDIOS FÍSICOS EN TRÁNSITO	34
ARTÍCULO 49. REGISTRO DE AUDITORÍA	34
CAPÍTULO VI CONTROL DE ACCESO ARTÍCULO 50. ADMINISTRACIÓN DE ACCESOS Y REGISTRO DE LOS USUARIOS	35
ARTÍCULO 51. ACCESO A LA ADMINISTRACIÓN DE LOS SISTEMAS OPERATIVOS.....	35
ARTÍCULO 52. MONITOREO DE ACCESOS	35
ARTÍCULO 53. LIMITACIÓN DEL TIEMPO DE USO DE APLICACIONES.....	35
ARTÍCULO 54. CATEGORÍAS Y PERFILES DE ACCESO	35
ARTÍCULO 55. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS	36
ARTÍCULO 56. CONTROL DE DISPOSITIVOS MÓVILES	36
ARTÍCULO 57. ACCESO AL CORREO ELECTRÓNICO	36
ARTÍCULO 58. ADMINISTRACIÓN DE CONTRASEÑAS	36
ARTÍCULO 59. EQUIPAMIENTO DESATENDIDO POR EL USUARIO	36
ARTÍCULO 60. POLÍTICA DE “MESA LIMPIA” Y “PANTALLA LIMPIA”	37
ARTÍCULO 61. TELETRABAJO	37

	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 7 de 46

CAPÍTULO VII ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	38
ARTÍCULO 62. AUTORIZACIÓN PARA ACCEDER NUEVOS RECURSOS DE PROCESAMIENTO DE INFORMACIÓN.....	38
ARTÍCULO 63. ESPECIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD.....	38
ARTÍCULO 64. SEPARACIÓN DE FUNCIONES DE LOS AMBIENTES	38
ARTÍCULO 65. ACCESO A LAS LIBRERÍAS DE SOFTWARE (APLICACIONES INFORMÁTICAS)	38
ARTÍCULO 66. CONTROL DE CAMBIOS DE SOFTWARE Y SISTEMAS DE INFORMACIÓN	39
ARTÍCULO 67. SUPERVISIÓN DEL DESARROLLO DE SOFTWARE POR TERCEROS	39
ARTÍCULO 68. LEGALIZACIÓN DE SOFTWARE	39
ARTÍCULO 69. PUBLICACIONES EN LA PÁGINA WEB.....	39
ARTÍCULO 70. RESPONSABILIDADES CON LA PÁGINA WEB	39
ARTÍCULO 71. ESTÁNDAR DE HARDWARE Y SOFTWARE	40
ARTÍCULO 72. POLÍTICA SOBRE ADQUISICIÓN DE HARDWARE Y SOFTWARE	40
CAPÍTULO VIII GESTIÓN DE INCIDENTES	41
ARTÍCULO 73. REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN E INCIDENTES	41
ARTÍCULO 74. ATENCIÓN A INCIDENTES INFORMÁTICOS POR DTIC	41
ARTÍCULO 75. RESPONSABILIDADES Y PROCEDIMIENTOS	41
ARTÍCULO 76. APRENDIENDO DE LOS INCIDENTES	41
ARTÍCULO 77. RECOLECCIÓN DE EVIDENCIA.....	41
CAPÍTULO IX GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	42
ARTÍCULO 78. INCLUYENDO LA SEGURIDAD DE LA INFORMACIÓN DENTRO DEL PROCESO DE ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO	42
ARTÍCULO 79. EVALUACIÓN DE RIESGOS Y CONTINUIDAD DEL NEGOCIO.....	42
ARTÍCULO 80. DESARROLLANDO E IMPLEMENTANDO PLANES DE CONTINUIDAD QUE TOMEN EN CUENTA LA SEGURIDAD DE LA INFORMACIÓN	42
ARTÍCULO 81. CONOCIMIENTO DE LOS ROLES Y RESPONSABILIDADES EN LA PLANIFICACIÓN DE CONTINGENCIAS Y RECUPERACIÓN DE SISTEMAS	42
ARTÍCULO 82. DEFINIR LA CLASIFICACIÓN DE RECUPERACIÓN DE LAS APLICACIONES.....	42
ARTÍCULO 83. PRUEBAS, MANTENIMIENTO Y RE EVALUACIÓN DE LOS PLANES DE CONTINUIDAD DE NEGOCIO.	43
CAPÍTULO X CUMPLIMIENTO	44
ARTÍCULO 84. IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE.....	44
ARTÍCULO 85. DERECHOS DE PROPIEDAD INTELECTUAL Y LEGALIZACIÓN DE SOFTWARE.....	44
ARTÍCULO 86. INFORMACIÓN DISPONIBLE DE FORMA PÚBLICA.....	44
ARTÍCULO 87 PREVENCIÓN CONTRA LA UTILIZACIÓN INDEBIDA DE LOS RECURSOS DE PROCESAMIENTO DE INFORMACIÓN	44
ARTÍCULO 88. ACCESO A INTERNET	44
ARTÍCULO 89 CREACIÓN DE BITÁCORAS Y LOGS DE AUDITORÍA	45
9 REFERENCIAS BIBLIOGRÁFICAS	46

1 INTRODUCCIÓN


El Ministerio de Trabajo y Seguridad Social siguiendo los lineamientos establecidos en las normativas y mejores prácticas internacionales define un marco de referencia para determinar directrices relacionadas con la Seguridad de la Información mediante la implementación de las políticas de Seguridad.

Estas políticas tienen como objetivo principal preservar las dimensiones de valoración de la Información: confidencialidad, disponibilidad, integridad de los datos, rendición de cuentas y trazabilidad por lo que en la Norma ISO/IEC 27001:2005 indica: “La información es un activo que, como otros activos importantes del negocio, es esencial para nuestra organización y requiere en consecuencia una protección adecuada. Esto es especialmente importante en ambientes de negocio cada vez más interconectados. Como consecuencia de este creciente íter conectividad, la información se expone a un número mayor y a una variedad más amplia de amenazas y vulnerabilidades.

La información adopta diversas formas. Puede estar impresa, almacenada electrónicamente, transmitida por correo o por medios electrónicos, proyectada o comunicada verbalmente. Sin importar la forma que tome la información o los medios por los que se comparte o almacene, la misma debe ser protegida adecuadamente.

La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se logra implantando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deben ser establecidos, implementados, supervisados, revisados y mejorados cuando fuere necesario para asegurar que se cumplen los objetivos específicos de la seguridad de información de la organización. Esto debe hacerse en forma conjunta con otros procesos de la administración del negocio.”

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 10 de 46

2 OBJETIVO

Brindar a las áreas y a los usuarios de Tecnologías de Información y Comunicación del Ministerio de Trabajo y Seguridad Social, un conjunto de lineamientos e instrucciones que permiten garantizar la seguridad en el ambiente informático, la información y demás recursos tecnológicos.


3 ALCANCE

Las políticas definidas en este documento deben ser de implementación obligatoria para todas aquellas Unidades Ejecutoras y Funcionarios que estén involucrados directa o indirectamente con el uso de tecnologías de información y comunicación.

4 CONSIDERACIONES GENERALES

- a- Este documento establece las políticas que se deben aplicar para mantener la seguridad de la información del MTSS.
- b- Seguridad de la información es la comprensión, conciencia y compromiso del personal del MTSS sobre la importancia de incorporar en sus prácticas cotidianas de gestión, un conjunto de controles (políticas y procedimientos) en ésta temática.
- c- El objetivo de la seguridad de la información es 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.
- d- El alcance de la seguridad de la información está definido por los recursos tecnológicos: datos, tecnología, aplicaciones, instalaciones y capital humano.
- e- El personal del MTSS está comprometido con la seguridad de la información que recibe, procesa, genera y almacena en su gestión.

- f- 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.
- g- La Administración Superior se compromete a apoyar la seguridad de la información mediante la promulgación, mantenimiento y divulgación de este manual
- h- Las premisas filosóficas de la seguridad de la información, que deben ser objeto de atención por la Administración Superior, son:
- Cumplimiento de la Misión del MTSS.
 - Apego al marco legal.
 - Asignación clara de responsabilidades funcionales y disciplinarias asociadas con el cumplimiento de las prácticas de seguridad de la información.
 - Relación costo-beneficio de los controles por diseñar.
 - Establecimiento de controles preventivos, correctivos y diagnósticos.
 - Monitoreo del ambiente de la organización y los cambios tecnológicos.
 - Educación al personal sobre conciencia de riesgo y seguridad, mediante charlas a los funcionarios regulares del Ministerio y a los de primer ingreso, tips de seguridad de la información enviados por correo. La Administración debe montar una campaña de divulgación que asegure que todos los funcionarios tengan conocimiento sobre el tema.
 - Fundamento en prácticas o estándares de aceptación general.
 - Fundamento en la valoración de riesgos a los que se exponen los recursos tecnológicos críticos.
 - Debe crearse un plan de divulgación y concienciación de la importancia de la seguridad de la información.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 12 de 46

5 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Una política de seguridad informática 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 informática no es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, la política de seguridad informática es una descripción de lo que deseamos proteger y él por qué de esta protección.

La política de seguridad informática está orientada a que cada uno de sus funcionarios de la Institución reconozca 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 deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

6 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros del Ministerio de Trabajo y Seguridad Social para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 13 de 46

- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. La autoridad responsable y las sanciones a aplicar ante cualquier falta estarán contenidas en el Reglamento Autónomo de Servicios de este Ministerio.

Las políticas de seguridad informática deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Las políticas de seguridad, deben revisarse periódicamente para ajustarlas de acuerdo a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de los servicios, entre otros.

7 CONTENIDO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las políticas de seguridad informática del MTSS se agrupan en los siguientes aspectos:


CAPÍTULO I- Políticas de Seguridad de la Información.

CAPÍTULO II- Políticas sobre Organización de Seguridad de la Información.

CAPÍTULO III- Políticas de Gestión de Activos.

CAPÍTULO IV- Políticas de Seguridad Física y del Ambiente.

CAPÍTULO V- Políticas de Gestión de Comunicaciones y Operaciones.

	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 14 de 46

CAPÍTULO VI- Políticas de Control de Accesos

CAPÍTULO VII- Políticas de Adquisición, desarrollo y mantenimiento de Sistemas de Información.

CAPÍTULO VIII – Políticas de Gestión de Incidentes de Seguridad de la Información

CAPÍTULO IX- Políticas de Gestión de la Continuidad del Negocio

CAPÍTULO X- Políticas de Cumplimiento

8 GLOSARIO

A

Activo: Aquello que tiene valor para la organización.

[ISO/IEC 13335-1:2004]

Hay muchos tipos de activos, incluyendo:


- a) información;
- b) software, tales como un programa de computador;
- c) físicos, como un computador;
- d) servicios;
- e) personas, y sus calificaciones, habilidades y experiencia, e
- f) intangibles, tales como la reputación y la imagen.

Acuerdo de Nivel de Servicio: Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

Ambiente de desarrollo: El ambiente de desarrollo se refiere a la utilización de paquetes computacionales que permiten elaborar sistemas de información que conformarán el ambiente de producción.

Los desarrolladores programan estos sistemas de información con equipos en principio lo más similares a los utilizados al ambiente de producción para simular las operaciones relacionadas con servicios que deberán atender con relación a los clientes internos y externos.

Ambiente de producción: El ambiente de producción es el conjunto de sistemas de información que permiten la gestión de toda organización mediante el uso de la computación para atender su necesidad de procesar su información y brindar atención a clientes internos y externos. Para que estos sistemas funcionen debe contarse con equipo de cómputo tal como computadoras de

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 16 de 46

escritorio, laptops y otros equipos similares, asimismo, se ocupan dispositivos de comunicación propios para esta labor.

Ambiente de pruebas: El ambiente de pruebas se refiere a los sistemas de información y a las pruebas, antes de ser puestos en un ambiente de producción. Las pruebas comprenden aspectos tal como: si funciona o no todas las partes del sistema de información y si se combinan exitosamente para brindar los resultados esperados.

A diferencia del ambiente de desarrollo, en este ambiente no es necesario ser un informático y es muy valiosa la participación de éste personal para corregir problemas relacionados con la funcionalidad o de programación para evitar el fracaso en el uso del sistema de información.

El ambiente de pruebas simula las condiciones bajo las cuales el sistema de información deberá estar trabajando cuando se instale en el ambiente de producción, lo cual implica simular cantidad de consultas simultáneas, ingreso de trámites, impresiones y otros aspectos operativos naturales para la unidad administrativa para la cual fue diseñado.


Aplicación: Cualquier software desarrollado o adquirido para un uso común y específico, por ejemplo el Microsoft Office, Auto CAD, programas utilitarios.

Autenticación de usuarios: Proceso mediante el cual un usuario es reconocido por una aplicación, sistema operativo o sistema de información, como usuario autorizado para tener acceso a la información que este administra.

B

Base de Datos: Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

Bitácora: Una bitácora es un archivo que registra información en forma cronológica, acerca de los eventos y acciones relacionados con un sistema, aplicación o base de datos, tales como fecha y hora de la acción, inclusión, modificación o borrado de datos y usuario que realiza la acción.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 17 de 46

La importancia de las bitácoras es la de contener información de utilidad, ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas, evidencia legal, es de gran ayuda en las tareas de cómputo forense

C

Código malicioso: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malicioso o malintencionado.

Confidencialidad de la información: Protección de información sensible contra divulgación no autorizada.

Control/Controles: Conjunto de acciones e instrumentos establecidos y oficializados para la verificación y seguimiento del cumplimiento de cada uno de los puntos que contempla la Política de Seguridad.

Control de Acceso: Los medios para garantizar que el acceso a los activos esté autorizado y restringido sobre la base de los requisitos del negocio y de la seguridad.


Continuidad del Negocio: Procesos y/o procedimientos para asegurarse de que las operaciones del negocio sean continuas.

Criticidad de la información/Aplicaciones: Indica el grado de necesidad que se tiene de la información. Se define en términos del tiempo mínimo tolerable durante el cual la información podría no estar disponible sin que afecte los objetivos del negocio.

Custodio de la Información: Es el responsable de monitorear que se cumplan las actividades encargadas de mantener la seguridad de la información.

D

Disponibilidad: Propiedad de ser accesible y utilizable según lo demande una entidad autorizada.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 18 de 46

DTI: Departamento de Tecnología de Información (Nombre del DTIC antes de la reorganización)

DTIC: Departamento de Tecnologías de Información y Comunicación

E

Excepción: Cualquier caso o situación que se dé y que no se encuentre contemplado específicamente dentro de los estándares, normativas, políticas o procedimientos.

G

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

[Orientación ISO/IEC 73:2002]

H


Hardware: Todos los componentes electrónicos, eléctricos y mecánicos que integran una computadora o cualquier dispositivo informático.

I

ID: Abreviación de 'identificativo', indica la identidad del usuario que desea acceder a un determinado sistema

Incidente de Seguridad de la Información: Evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones y amenazar la Seguridad de la información.

[ISO/IEC TR 18044:2004]

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 19 de 46

Impacto: Cambio adverso en el nivel de los objetivos de negocio alcanzados.

L

Lineamiento: Orden o directriz.

Log: Registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática un log es usado para registrar datos o información sobre quién, que, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

M

MTSS: Ministerio de Trabajo y Seguridad Social

P


Perfil de acceso: Definición particular de autorizaciones o restricciones que se asocia a un usuario de un sistema de información específico de acuerdo con las funciones que el usuario desempeña.

Procedimiento: Conjunto de pasos, instrucciones y controles establecidos para llevar a cabo una tarea.

Programa fuente: Código fuente de las aplicaciones o sistemas de información que ha sido entregado por el desarrollador a la institución.

Propietario de la información: Es la persona responsable de verificar la integridad de la información a su cargo y de velar que se mantenga la confidencialidad y disponibilidad de esa información.

Proveedor: Persona física o jurídica contratada por el Ministerio para proveer servicios en el ámbito de TIC.

	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 20 de 46

R

Riesgo: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la institución.

Rol: Función específica que alguien cumple.

S

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 27002:2008]

Seguridad física: Protección física del hardware, software, instalaciones y personal relacionado con los sistemas de información.


Seguridad lógica: Conjunto de controles de TIC para promover la confidencialidad, integridad y disponibilidad de la información.

Software: Los programas y la documentación que los soporta y que permiten y facilitan el uso de la computadora.

Software malicioso: Malware (del inglés malicious software), también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

T

Teletrabajo: Según lo establecido en el artículo IV del decreto 34704-MP-MTSS, “el teletrabajo es una nueva modalidad de organización de la prestación laboral, basada en las tecnologías de la información, que supone importantes beneficios para el país al fomentar la reducción del consumo del combustible, impacto positivo en el medio ambiente, para la organización al exigir la identificación de objetivos y la evaluación del grado de su cumplimiento, para los propios

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 21 de 46

funcionarios que al desempeñar total o parcialmente su jornada de trabajo desde su domicilio o lugar habilitado, ven aumentadas sus posibilidades de conciliación del desarrollo profesional con su vida personal y laboral.

Terceros: Personas o empresas contratadas para desarrollar, implementar, instalar o dar mantenimiento al hardware y software del Ministerio de Trabajo.

Tecnologías de Información y Comunicación: Conjunto de tecnologías dedicado al manejo de la información institucional y de su transmisión. Incluye los recursos de hardware, software, infraestructura, comunicación y personas.


Tipo de información: Clase o naturaleza de información incluyendo la manera en que se guarde o soporte.

U

Usuarios finales: En informática el término usuario final designa a la persona o personas que van a manipular de manera directa un producto de software.

V

Vulnerabilidad: En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 22 de 46

9 DESCRIPCIÓN DE LAS POLITICAS

CAPÍTULO I POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 1. COMPROMISO DE LA ADMINISTRACIÓN CON LA SEGURIDAD DE LA INFORMACIÓN

La Administración Superior es responsable de apoyar la gestión de Seguridad de la Información y proveer los recursos necesarios para la implementación de estas políticas, garantizando que todas las Dependencias del Ministerio cumplan con la misma, de acuerdo a lo establecido en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información N-2-2007-CO-DFOE.

ARTÍCULO 2. DOCUMENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Estas políticas son de cumplimiento obligatorio para todos los funcionarios del Ministerio que utilicen tecnologías y servicios provistos por el Departamento de Tecnología de Información y Comunicación (en adelante DTIC), una vez hayan sido oficializadas por los niveles jerárquicos correspondientes del MTSS.

ARTÍCULO 3. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Jefatura del Departamento de Tecnologías de Información y Comunicación y la Unidad de Seguridad Informática, Gestión de la Calidad y Riesgos deben realizar una revisión de las políticas de Seguridad mínimo una vez al año.

ARTÍCULO 4. 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 complemento con el Sistema Específico de Valoración de Riesgo (SEVRI), en el cual se deben establecer las directrices para el manejo del riesgo involucrado. La Administración Superior comunicará este plan a quienes considere necesario.

ARTÍCULO 5. SEGURIDAD INFORMÁTICA EN EL PLAN ANUAL OPERATIVO

El DTIC en coordinación con la Administración Superior debe incluir en el Plan Anual Operativo (PAO) del MTSS el cual está alineado con el Plan Estratégico de Tecnologías de Información (PETI) las mejoras relativas a la Seguridad Informática.


ARTÍCULO 6. INCLUSIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PLAN ANUAL DEL MTSS

La Administración Superior debe incluir en el Plan Anual Operativo, en el Plan Estratégico del MTSS y en el Plan Estratégico de Tecnología de Información, los requisitos de Seguridad de la

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 23 de 46

Información necesarios para garantizar la continuidad operacional de la Institución. El DTIC semestralmente debe revisar los derechos otorgados a los usuarios de la red y diferentes sistemas de información de la Institución con el fin de garantizar que los accesos correspondan estrictamente al necesario para el ejercicio de sus funciones.

La Administración Superior TIC tiene la potestad, de suspender en cualquier momento los accesos a los recursos de Tecnologías de Información, en caso de comprobarse el mal uso de estos privilegios.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 24 de 46

CAPÍTULO II ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 7. DIVULGACIÓN Y PROMOCIÓN

La Administración Superior debe divulgar y promover el tema de Seguridad de la Información, para que en forma clara y breve se describan las políticas, estándares y procedimientos de la seguridad de información en el MTSS, con el fin de inculcar en los funcionarios la cultura de la Seguridad de Información. El DTIC es el responsable de proporcionar a la Administración Superior el material necesario que debe ser divulgado.

ARTÍCULO 8. DEFINICIÓN DE LAS RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN

La Administración Superior es responsable de garantizar que en el Manual Descriptivo de Cargos del Ministerio de Trabajo y Seguridad Social de todos los funcionarios y en el Reglamento Autónomo existan responsabilidades en función de Seguridad de la Información.

El DTIC debe dar el seguimiento oportuno sin intervenir en las funciones propias de la Auditoría a todas las transgresiones a esta política de seguridad que se detecten y comunicar a la jefatura inmediata los hallazgos, para que ésta tome las medidas correctivas correspondientes según el Reglamento Autónomo. Cuando sea considerado necesario se llevará acabo revisiones aleatorias sin previo aviso del cumplimiento de estas políticas.


ARTÍCULO 9. USO DE HERRAMIENTAS INFORMÁTICAS

Es responsabilidad de todos los funcionarios del Ministerio utilizar todos los sistemas licenciados y de software libre provistos y autorizados por el DTIC, para desempeñar sus labores en la institución.

ARTÍCULO 10. ACUERDOS DE CONFIDENCIALIDAD

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 un 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.

	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 25 de 46

ARTÍCULO 11. CONTACTOS CON GRUPOS DE INTERÉS

Todos los funcionarios de DTIC deben participar en foros sobre temas de Seguridad de la Información para mantener actualizado su conocimiento y ser apoyo estratégico al MTSS. El Departamento de Gestión de Capital Humano deberá coordinar lo correspondiente para la asistencia de dichos funcionarios.

ARTÍCULO 12. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN Y CONTROLES DE AUDITORÍA PARA SISTEMAS DE INFORMACIÓN


La Dirección General de Auditoría debe planificar de forma anual revisiones aleatorias a las políticas, procedimientos y objetivos de control de la Seguridad de la Información, así como validación del cumplimiento técnico y cumplimientos con regulaciones locales e internacionales.

ARTÍCULO 13. IDENTIFICACIÓN DE RIESGOS RELACIONADOS CON ENTIDADES EXTERNAS

El DTIC debe supervisar todo acceso, físico o lógico que requiera un tercero para hacer uso de recursos de Tecnologías de Información y Comunicación, con el objetivo de identificar, evaluar e implementar los controles necesarios para minimizar la exposición a los riesgos.

ARTÍCULO 14. DIRIGIENDO LA SEGURIDAD AL REALIZAR ACUERDOS CON TERCEROS

La Proveeduría Institucional debe garantizar que toda licitación o adquisición de equipo (hardware) o software que se realiza a proveedores debe considerar los requerimientos proporcionados por el DTIC y acordados con el encargado o representante del proyecto.

	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 26 de 46

CAPÍTULO III GESTIÓN DE ACTIVOS

ARTÍCULO 15. INVENTARIO DE ACTIVOS

El Área de Control de Activos de la Proveeduría Institucional debe identificar, etiquetar y registrar claramente todos los activos informáticos, tanto tangibles como intangibles (hardware y software), los cuales deben ser asignados a los funcionarios de la Institución de acuerdo a lo que establece el Reglamento de Registro y Control de los Bienes de la Administración Central.

La Proveeduría Institucional debe remitir al DTIC toda la información registrada en el Sistema de Control de Activos (SIBINET), referente al inventario de hardware y software, al menos 1 vez al año, sin perjuicio de que el DTIC mantenga un control permanente y actualizado de esta información sobre estos activos como condición necesaria para una óptima gestión de sus servicios y el cumplimiento de sus responsabilidades.

El DTIC es responsable de realizar todo el inventario de todo el equipo informático y el licenciamiento del software instalado, los sistemas de información y las bases de datos contenidas en la plataforma tecnológica y, en el caso de los activos patrimoniales, deberá confrontar esa información, al menos una vez al año, con el reporte de activos suministrado por la Proveeduría Institucional.

ARTÍCULO 16. IDENTIFICACIÓN DEL PROPIETARIO Y CUSTODIO DE CADA TIPO DE INFORMACIÓN

Todas las dependencias son dueñas de la información (datos e información) que utilicen y generen para el ejercicio de su función, por lo cual son responsables de la integridad y confidencialidad de la misma.

El DTIC debe custodiar y administrar la información de las bases de datos, aplicaciones y sistemas, así como los servidores principales que las soportan, ubicados en el Data Center, siendo responsable de los aspectos técnicos y definición de controles para la protección de los mismos.

El DTIC debe tener identificado al propietario de la información de las Bases de Datos, aplicaciones y sistemas de información.

ARTICULO 17. USO ACEPTABLE DE LOS ACTIVOS

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.

Es responsabilidad del funcionario administrar, mantener y cuidar la seguridad de los activos de información (Hardware, Software, equipos auxiliares, instalaciones entre otros) los cuales le son asignados para uso exclusivo de sus actividades laborales.

Los funcionarios del Ministerio son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Institución sobre la importancia y valor de esa información y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios del Ministerio no deben agregar, modificar o borrar software, información, bases de datos o registros del Ministerio, realizar cualquier daño a los equipos o a la información, las configuraciones de sistemas operativos o los aplicativos que se encuentren en ellos instalados; revelar o compartir contraseñas de acceso, propias o de terceros, así como el uso de la identificación, identidad, firma electrónica o digital propia o de otro usuario; utilizar el sistema de correo o cualquier tipo de comunicación electrónica con el propósito de revelar información privada de otras personas; lanzar cualquier tipo de virus o programa de computación con el fin de impactar el funcionamiento de los diferentes servicios provistos por el Ministerio internos o externos; realizar cualquier actividad contraria a los intereses del Ministerio, tal como publicar información reservada, acceder sin autorización a los servicios informáticos o impedir el acceso a los mismos; alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación u otros documentos o propiedades; descargar, almacenar, instalar o publicar cualquier material de actividad contraria a los intereses del Ministerio, a través de los recursos informáticos brindados por la Administración Superior.


ARTÍCULO 18. DIRECTRICES DE CLASIFICACIÓN, ETIQUETADO Y MANEJO DE INFORMACIÓN

Todo activo de Información, que administre el DTIC debe de ser etiquetado de acuerdo a lo indicado por las dependencias del Ministerio las cuales son las dueñas de esa información, a saber: Datos de acceso restringido, Datos de acceso irrestricto, Datos sensibles.

ARTÍCULO 19. DEVOLUCIÓN DE ACTIVOS

Con el asesoramiento de la Proveeduría Institucional, el funcionario y usuario externo deben entregar a su jefe inmediato o al responsable del Programa dueño del equipo, al término de la relación laboral, contrato o acuerdo, o al DTIC cuando se requieran cambios de equipo que lo ameriten, los activos, ya sean estos tangibles o intangibles, tales como hardware, software asignados para el cumplimiento de sus labores así como la información (informes, manuales, formularios, etc.) generada durante la relación laboral con el MTSS.

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 respectiva.


 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 28 de 46

ARTÍCULO 20. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

El DTIC es responsable de revocar cualquier acceso a los servicios informáticos una vez finalizada la relación laboral del funcionario o cambio de puesto. El Departamento de Gestión de Capital Humano debe remitir la comunicación respectiva a la mayor brevedad.

ARTÍCULO 21. AVISOS DE VULNERABILIDADES

El DTIC es responsable de revisar los avisos de vulnerabilidades emitidos por las organizaciones internacionales y realizar las recomendaciones que estimen necesarias para garantizar la correcta operación de los recursos tecnológicos a nivel institucional.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 29 de 46

CAPÍTULO IV SEGURIDAD FÍSICA Y DEL AMBIENTE

ARTÍCULO 22. PERÍMETRO DE SEGURIDAD FÍSICA

Los funcionarios y la Administración Superior deben garantizar que todos los activos de información estén 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.

ARTÍCULO 23. ACCESO A LOS ARCHIVOS Y DOCUMENTOS FÍSICOS

Todas las Dependencias del Ministerio deben restringir el acceso a los documentos físicos bajo su custodia cuando así lo considere conveniente para sus intereses o del Ministerio.

ARTÍCULO 24. CONTROLES DE ACCESO FÍSICO

La Administración Superior en coordinación con el DTIC, debe definir e implementar controles robustos 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.


ARTÍCULO 25. SEGURIDAD DE OFICINAS, DESPACHOS E INSTALACIONES

Las instalaciones de acceso restringido deben estar ubicadas de manera que eviten el acceso al público.

Las áreas de acceso restringido deben permanecer cerradas bajo llave o con dispositivo de control. Se debe evitar dejar sin atención las oficinas ubicadas en áreas restringidas en horas laborales.

ARTÍCULO 26. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES

La Administración Superior debe garantizar que el equipo informático, medios de respaldo y cableado eléctrico y telecomunicaciones que da soporte a la operativa del Ministerio de Trabajo se encuentren ubicados de forma tal que esté protegido 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.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 30 de 46

ARTÍCULO 27. CAMBIOS EN ESPACIO FÍSICO

Las Dependencias 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.

ARTÍCULO 28. TRABAJO EN ÁREAS SEGURAS

Todos los funcionarios que ingresen al área de informática deben portar identificación visible o ser acompañados por un funcionario del Ministerio identificado.

Todo proveedor de servicios o persona ajena al MTSS debe estar siempre acompañado por el funcionario encargado, con el fin de supervisar su trabajo y evitar daños a la infraestructura o datos.

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, con el fin de detectar salidas de equipo no autorizadas.

ARTÍCULO 29. ÁREAS DE ACCESO PÚBLICO

La Administración Superior es responsable de emitir las directrices que aseguren, eviten y controlen el ingreso no autorizado a los datos, información y equipos tecnológicos, en las áreas del Ministerio que son de acceso al público general


ARTICULO 30. MANTENIMIENTO DEL EQUIPO

La Administración Superior debe garantizar que todo equipo custodiado por los funcionarios del Ministerio, del DTIC o que sea un recurso para mantener la operativa del cuarto de servidores, a saber: hardware, elementos de soporte (aprovisionamiento eléctrico, UPS, Aire acondicionado), deben recibir 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.

ARTICULO 31. SEGURIDAD DEL EQUIPO FUERA DE SITIO

Tanto DTIC como los funcionarios del MTSS deben garantizar que todo equipo del Ministerio que con fines laborales se encuentre fuera de la institución, debe contar con todas las medidas de seguridad adecuadas para prevenir de daño o hurto, asegurando así la confidencialidad, fidelidad y disponibilidad de la información.


 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 31 de 46

ARTÍCULO 32. 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 que todo equipo que contenga medios de almacenamiento 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.

ARTÍCULO 33. 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.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 32 de 46

CAPÍTULO V GESTIÓN DE COMUNICACIONES Y OPERACIONES

ARTÍCULO 34. DOCUMENTACIÓN DE LOS PROCEDIMIENTOS DE OPERACIÓN

El DTIC debe documentar debidamente todos los procedimientos de operación necesarios para el desempeño de las funciones del Departamento.

ARTÍCULO 35. ACTUALIZACIONES DE SEGURIDAD Y CAMBIOS

El DTIC debe identificar, registrar, mantener e implementar todas las actualizaciones o cambios necesarios para el sistema operativo, hardware, aplicaciones, prestación de servicios, o cambios de seguridad, las cuales deben ser evaluadas por el funcionario encargado considerando el impacto, priorización y autorización. En caso de ser provisto por un tercero, debe ser supervisado, con el fin de asegurar la información del MTSS.

La unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del DTIC debe garantizar que toda instalación o actualización de Software, respete los estándares y requerimientos de las aplicaciones instaladas en el MTSS.

ARTÍCULO 36. SEGREGACIÓN DE FUNCIONES

Es responsabilidad de la jefatura de DTIC en conjunto con la Administración Superior, garantizar que la asignación de responsabilidades del Departamento, no presente conflictos de segregación de funciones, esto con el fin de reducir la probabilidad de que se presenten errores, ya sea intencionales o involuntarios.

ARTÍCULO 37. ACCESO AL AMBIENTE DE PRODUCCIÓN


El DTIC debe autorizar y controlar el acceso al ambiente de producción únicamente a los usuarios involucrados en el sistema o aplicación de su competencia.

ARTÍCULO 38. GESTIÓN DE LA CAPACIDAD

El DTIC debe realizar en conjunto con la Administración Superior y en alineamiento con el PEI y PETI, 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.

ARTÍCULO 39. PROTECCIÓN CONTRA CÓDIGO MALICIOSO

La unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del DTIC debe implementar controles de detección, prevención y recuperación, con el fin de protegerse de código malicioso.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 33 de 46

ARTÍCULO 40. RESPALDO (BACKUP)

La Administración Superior en conjunto con el DTIC, debe implementar los controles necesarios para el cumplimiento de los artículos 1, 2, 6, 7, 16,17, y el capítulo III de la presente, considerando la generación de respaldos de toda la información necesaria para las operaciones del MTSS, y en acatamiento de lo dispuesto en la directriz 29-2007 del 14/11/2007 emitida por la Junta Administrativa del Archivo Nacional.

La ubicación de los respaldos (Backups) debe contar con adecuadas medidas de seguridad, al menos una copia de los respaldos debe almacenarse en el exterior del MTSS y los mismos deben ser transportados en un medio seguro que los proteja. Debe designarse un responsable y un suplente encargados de su custodia o bien, si los respaldos se realizan en la nube, deben asegurar que los mismos se hacen sin ningún problema y deben llevar un registro de los movimientos en cualquiera de estos medios.

ARTÍCULO 41. RESPALDO DE DOCUMENTOS CON FIRMA DIGITAL

La Administración Superior en conjunto con el DTIC deben garantizar a los funcionarios del MTSS que utilizan la firma digital de documentos, un espacio en un ambiente seguro y todas las condiciones necesarias, para el respaldo de ese tipo de documentos.

ARTÍCULO 42. RETENCIÓN DE INFORMACIÓN


La Administración Superior en conjunto con el DTIC deben garantizar que los procesos de respaldo y retención de información en medios digitales en acatamiento a las directriz 29-2007 del 14/11/2007 emitida por la Junta Administrativa del Archivo Nacional tomen en cuenta los períodos de retención y almacenamiento considerando los requerimientos regulatorios establecidos.

ARTÍCULO 43. ADMINISTRACIÓN DE CONTROLES DE ACCESO A LA RED

La Unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del 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.

ARTÍCULO 44. IDENTIFICACIÓN DEL EQUIPO EN LA RED

El DTIC debe garantizar que todos los equipos conectados a la red institucional estén correctamente identificados, para facilitar la administración desde equipos y ubicaciones específicas.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 34 de 46

ARTÍCULO 45 SEGMENTACIÓN DE REDES

La Unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del 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.

ARTÍCULO 46. COMPUTACIÓN MÓVIL Y COMUNICACIONES

La Unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del DTIC, debe establecer las medidas de seguridad adecuadas para evitar los riesgos en caso de utilizar medios de computación y comunicación móvil. Estas medidas se deben extender a la utilización segura y eficiente de redes inalámbricas.

ARTÍCULO 47. INTERCAMBIO DE INFORMACIÓN

La Administración Superior y el DTIC deben establecer las directrices para el intercambio de información a nivel institucional e interinstitucional, según la clasificación dada a la misma tomando en cuenta el grado de criticidad y la información expuesta.

ARTÍCULO 48. MEDIOS FÍSICOS EN TRÁNSITO

El DTIC debe recomendar que el transporte de medios físicos fuera de las instalaciones del Ministerio sea con las correspondientes medidas de seguridad considerando la clasificación de la información.

ARTÍCULO 49. REGISTRO DE AUDITORÍA

Se prohíbe a todos los funcionarios alterar o borrar bitácoras de los **recursos de TI**. Cualquier excepción, únicamente por motivos de rendimiento o espacio de almacenamiento en el equipo, debe ser aprobada por escrito por el Jefe de DTIC y se debe respaldar la bitácora antes de eliminarla.

CAPÍTULO VI CONTROL DE ACCESO

ARTÍCULO 50. ADMINISTRACIÓN DE ACCESOS Y REGISTRO DE LOS USUARIOS

El Director o Jefe será responsable de solicitar de forma escrita al DTIC la creación, suspensión, cambio y revocación de los privilegios sobre el uso de los recursos de Tecnología de Información de los usuarios de su área, basándose en los principios de necesidad de conocer.

La Administración Superior tiene la potestad, de suspender en cualquier momento los accesos a la plataforma tecnológica, en caso de comprobarse el mal uso de estos privilegios.

El DTIC debe revisar 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 estrictamente al necesario para el ejercicio de sus funciones.

ARTÍCULO 51. ACCESO A LA ADMINISTRACIÓN DE LOS SISTEMAS OPERATIVOS

La Unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del DTIC, debe restringir el acceso a los sistemas operativos y servidores de manera que solo los funcionarios asignados ejecuten esas funciones. (Relación con artículos 91 y 92).

ARTÍCULO 52. MONITOREO DE ACCESOS

El DTIC debe controlar y monitorear los accesos a los sistemas de información, aplicaciones, servidores y páginas web periódicamente, con el fin de identificar potenciales usos inapropiados.


ARTÍCULO 53. LIMITACIÓN DEL TIEMPO DE USO DE APLICACIONES

El DTIC debe restringir el acceso a los sistemas de información y la utilización de recursos informáticos del MTSS, en un rango de horario definido.

ARTÍCULO 54. CATEGORÍAS Y PERFILES DE ACCESO

El Propietario de la información (Dependencias o Unidades) tiene a su cargo el establecimiento, definición y aprobación de los funcionarios y sus perfiles de acceso a los sistemas de información.

La Unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del DTIC debe asignar los permisos para acceder la información o partes de ésta, basándose en esos perfiles definidos por las Dependencias.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 36 de 46

ARTÍCULO 55. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS

La Unidad de Infraestructura, Telecomunicaciones y Soporte Técnico del DTIC, debe asignar a los funcionarios que deban ingresar a la red informática institucional, que utilicen los sistemas y aplicaciones, un identificador único (usuario) el cual será de uso exclusivo, de manera que las acciones que realice en dicha red sean auditables.

El uso de cuentas genéricas, no está permitido en la infraestructura tecnológica del Ministerio.

ARTÍCULO 56. CONTROL DE DISPOSITIVOS MÓVILES

EL DTIC debe implementar procedimientos que garanticen la seguridad de la información en caso de utilizar dispositivos móviles (computadoras portátiles, memorias USB, discos externos provistos por el Ministerio), de manera que se garantice la operación de los dispositivos y no se comprometa la información de la Institución.

ARTÍCULO 57. ACCESO AL CORREO ELECTRÓNICO

El DTIC es responsable de crear o liberar (eliminar) las cuentas de correo electrónico institucional cuando así corresponda.

ARTÍCULO 58. ADMINISTRACIÓN DE CONTRASEÑAS

El DTIC es responsable de crear los usuarios de los funcionarios para el ingreso a los recursos o sistemas informáticos del Ministerio.

Los funcionarios del Ministerio son responsables de cambiar sus contraseñas para el acceso a estos recursos cuando así sea requerido.


Estas contraseñas deben ser difíciles de suponer o adivinar, no deben incluir información como su nombre, no deben usar la misma contraseña para propósitos particulares, son confidenciales, no deben ser compartidas con otras personas, no deben ser apuntadas en cuadernos o lugares que sean de fácil acceso para otras personas.

ARTÍCULO 59. EQUIPAMIENTO 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).

El DTIC debe habilitar un mecanismo automático para bloqueo del equipo, por ejemplo un protector de pantalla protegido con contraseña.

Todo funcionario al finalizar de su jornada laboral y en fines de semana, debe apagar la computadora, pantalla y todo equipo de oficina que no requiera estar activo.

	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 37 de 46

ARTÍCULO 60. POLÍTICA DE “MESA LIMPIA” 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.

ARTÍCULO 61. TELETRABAJO

Es responsabilidad de la Administración Superior, Departamento de Gestión de Capital Humano y DTIC, implementar controles administrativos y técnicos, así como asignación de responsabilidades para la protección de la información cuando se realizan actividades de teletrabajo.

CAPÍTULO VII ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

ARTÍCULO 62. AUTORIZACIÓN PARA ACCEDER NUEVOS RECURSOS DE PROCESAMIENTO DE INFORMACIÓN

Ninguna Dirección, Dependencia o Organismo externo al Ministerio **deben** donar, desarrollar o implementar Sistemas de Información sin el aval y consentimiento del DTIC.

Todo nuevo sistema que nace como necesidad del negocio y el cual el DTIC debe administrar, modificar o dar soporte debe cumplir con la metodología para el desarrollo de sistemas, la metodología de gestión de proyectos, la definición de los niveles de servicio, capacitación y aceptación del mismo.

A nivel estratégico el Comité Informático Institucional en conjunto con la Administración Superior, deben aprobar cada nueva instalación de Tecnología de Información.

A nivel técnico la jefatura de DTIC debe aprobar cada nueva instalación de Tecnología de Información.

ARTÍCULO 63. ESPECIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD

Los requerimientos de seguridad deben ser establecidos por el DTIC para cualquier ciclo del desarrollo de sistemas y tanto para un sistema nuevo como para una modificación o mejora a sistemas existentes.


ARTÍCULO 64. SEPARACIÓN DE FUNCIONES DE LOS AMBIENTES

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 en este punto.

ARTÍCULO 65. ACCESO A LAS LIBRERÍAS DE SOFTWARE (APLICACIONES INFORMÁTICAS)

La jefatura de DTIC debe nombrar un funcionario del departamento que se encargue de la custodia de los programas 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.

El encargado de la custodia debe garantizar que los programas fuente y la documentación respaldada siempre sean las versiones que se encuentren en producción. Además debe constituir un histórico de esas versiones.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 39 de 46

ARTÍCULO 66. CONTROL DE CAMBIOS DE SOFTWARE Y SISTEMAS DE INFORMACIÓN

El DTIC debe crear un comité de cambios de TI conformado por representantes de cada unidad funcional.

El DTIC debe implementar un procedimiento de control de cambios.

ARTÍCULO 67. SUPERVISIÓN DEL DESARROLLO DE SOFTWARE POR TERCEROS

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 aplique la metodología de desarrollo de sistemas establecida, cumpla con los requisitos de seguridad y los requerimientos 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.

ARTÍCULO 68. LEGALIZACIÓN DE SOFTWARE

El DTIC debe garantizar la adquisición y uso adecuado de todos los programas de cómputo y la protección del derecho de autor de los mismos para cumplir con lo establecido en el decreto de Legalización de Software 30.151-J.

Igualmente las empresas contratadas para el desarrollo de aplicaciones deben cumplir lo establecido en esta política.


ARTÍCULO 69. PUBLICACIONES EN LA PÁGINA WEB

Toda publicación en cualquiera de las secciones de la página web del MTSS debe estar aprobados por el Director de la dependencia dueña de la información y la Oficina de Prensa del Ministerio.

Los contenidos a publicar deben respetar los estándares establecidos, conservando su homogeneidad en diseño y estructura. Esta publicación puede ser, imágenes, archivos PDF, archivos de Microsoft Office, archivos XML, archivos de video o archivos de audio; deben ser de fácil uso, claros, precisos y de lenguaje sencillo; igualmente deben tratar temas vigentes, relevantes, verificables y completos. En el caso de las imágenes o videos, estos deben ser estéticos y ser congruentes con las funciones sustantivas y leyes del MTSS.

ARTÍCULO 70. RESPONSABILIDADES CON LA PÁGINA WEB

El funcionario encargado de administrar las redes sociales asociados a la página web debe garantizar que todo lo que se publique en ellas cumpla con lo establecido en esta política.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 40 de 46

ARTÍCULO 71. ESTÁNDAR DE HARDWARE Y SOFTWARE

La Jefatura del DTIC debe recomendar que toda adquisición de hardware y software que adquiera la Institución cumpla con los estándares y los requerimientos establecidos para la compra de los mismos y debe hacerse a través de la Proveeduría Institucional

Es responsabilidad del Director del Programa Presupuestario y de la Proveeduría Institucional acatar la recomendación establecida por el DTIC para la adquisición de hardware y software.


ARTÍCULO 72. POLÍTICA SOBRE ADQUISICIÓN DE HARDWARE Y SOFTWARE

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 evalúe 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.

	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 41 de 46

CAPÍTULO VIII GESTIÓN DE INCIDENTES

ARTÍCULO 73. REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN E INCIDENTES

Los funcionarios deben de reportar todos los incidentes y solicitudes de servicios informáticos en la herramienta provista por el DTIC.

Es responsabilidad del funcionario del Ministerio que tramitó el incidente aceptar o rechazar la conclusión del mismo.

ARTÍCULO 74. ATENCIÓN A INCIDENTES INFORMÁTICOS POR DTIC

El DTIC tiene la responsabilidad de organizar y mantener un equipo para la atención de incidentes informáticos.

Este equipo tendrá el compromiso de brindar una respuesta organizada y ágil a las solicitudes, incidentes y problemas.

ARTÍCULO 75. RESPONSABILIDADES Y PROCEDIMIENTOS

El DTIC debe establecer una gestión de atención de incidentes, solicitudes y problemas. Estos incidentes deben ser documentados para crear una base de datos de conocimiento y se debe cumplir el seguimiento oportuno de los mismos.


El DTIC pondrá a disposición de todos los funcionarios del Ministerio un Sistema para la gestión de incidentes, solicitudes y problemas.

ARTÍCULO 76. APRENDIENDO DE LOS INCIDENTES

El coordinador de la Unidad de Seguridad Informática Gestión de Calidad y Riesgo o a quien la Jefatura del DTIC designe para tal caso, debe realizar un análisis de los principales problemas presentados en el Ministerio con respecto a las incidencias incurridas, comunicándolo a la Jefatura del DTIC, mediante un informe con copia a la Administración Superior.

ARTÍCULO 77. RECOLECCIÓN DE EVIDENCIA

EL DTIC debe colaborar y apoyar ante un incidente que involucre causas legales a recopilar la información de forma íntegra.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 42 de 46

CAPÍTULO IX GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

ARTÍCULO 78. INCLUYENDO LA SEGURIDAD DE LA INFORMACIÓN DENTRO DEL PROCESO DE ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

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.

ARTÍCULO 79. EVALUACIÓN DE RIESGOS Y CONTINUIDAD DEL NEGOCIO

El DTIC en conjunto con los propietarios de los sistemas de información y con la Administración Superior, debe realizar un análisis del impacto que tendría para la Institución operar sin la información crítica.

El DTIC debe realizar una evaluación de riesgos en la que como producto se especifique el tiempo en que la institución puede trabajar sin la información crítica, el periodo de tiempo que se debe dar antes de iniciar a trabajar bajo el plan de contingencia y cuál es la configuración mínima aceptable para operar con este plan. Tomando como base, la metodología de control interno del MTSS (SEVRI-MTSS).

ARTÍCULO 80. DESARROLLANDO E IMPLEMENTANDO PLANES DE CONTINUIDAD QUE TOMEN EN CUENTA LA SEGURIDAD DE LA INFORMACIÓN


El DTIC y las Dependencias del Ministerio son responsables de establecer, implementar y actualizar los planes de contingencia y sus procedimientos en caso de una interrupción o degradación del servicio, con el fin de recuperar y restaurar las operaciones del MTSS.

ARTÍCULO 81. CONOCIMIENTO DE LOS ROLES Y RESPONSABILIDADES EN LA PLANIFICACIÓN DE CONTINGENCIAS Y RECUPERACIÓN DE SISTEMAS

Los roles, las responsabilidades y los procedimientos de recuperación de sistemas indicados en el plan de contingencias deben ser revisados una vez al año como mínimo, por el o los funcionarios del DTIC definidos por la jefatura del Departamento en conjunto con las Dependencias, quienes deben realizar las observaciones que estimen pertinentes para mantener el plan actualizado y garantizar su éxito en caso de ser aplicado.


ARTÍCULO 82. DEFINIR LA CLASIFICACIÓN DE RECUPERACIÓN DE LAS APLICACIONES

El Comité Informático y/o las Dependencias del MTSS en coordinación con el DTIC, deben elaborar un esquema de clasificación de los recursos de Tecnologías y sistemas de Información y dar la prioridad de recuperación de cada uno en caso de emergencia.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 43 de 46

ARTÍCULO 83. PRUEBAS, MANTENIMIENTO Y RE EVALUACIÓN DE LOS PLANES DE CONTINUIDAD DE NEGOCIO.

El DTIC y las Dependencias tienen la responsabilidad de evaluar y actualizar regularmente los planes de continuidad, para garantizar su efectividad.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 44 de 46

CAPÍTULO X CUMPLIMIENTO

ARTÍCULO 84. IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE.

El DTIC debe 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.

ARTÍCULO 85. DERECHOS DE PROPIEDAD INTELECTUAL Y LEGALIZACIÓN DE SOFTWARE

La Administración Superior en conjunto con el DTIC deben garantizar la adquisición y velar por el uso adecuado de los programas de cómputo y la protección del derecho de autor de los mismos cumpliendo sin excepción con el Decreto No. 30.151-J del 1 de febrero del 2002 Reglamento de Protección al Software en el Gobierno Central y con el Reglamento Nº 37549 Reglamento Para la Protección de Equipos de Cómputo del 26 de noviembre del 2012, relacionados con la Ley Nº 6683 de Derechos de Autor y Derechos Conexos y la Ley Nº 8039 sobre Procedimientos de Observancia de los Derechos de Propiedad Intelectual, tanto para proveedores como para uso interno.

Los funcionarios del Ministerio no deben acceder, descargar, transmitir, distribuir o almacenar videos, música, imágenes, documentos y/o cualquier otro software o archivo protegido por las normas de propiedad intelectual.

ARTÍCULO 86. INFORMACIÓN DISPONIBLE DE FORMA PÚBLICA


El MTSS debe proteger la información en los sistemas que puede ser accesada públicamente, aplicando las regulaciones locales sobre la protección de datos personales.

ARTÍCULO 87 PREVENCIÓN CONTRA LA UTILIZACIÓN INDEBIDA DE LOS RECURSOS DE PROCESAMIENTO DE INFORMACIÓN

Todas los recursos de procesamiento incluyendo pero no limitado a correo electrónico, aplicaciones, impresoras, faxes son proporcionadas a los colaboradores para propósitos exclusivos del Ministerio, los mismos no deben ser utilizadas para fines personales.


ARTÍCULO 88. ACCESO A INTERNET

El acceso a internet para los funcionarios del MTSS deberá ser para uso estrictamente laboral (ejemplo: no se puede bajar música, ver o bajar videos, jugar en línea, acceder a páginas de entretenimiento, entre otras) y debe ser solicitado por el jefe inmediato del funcionario y será asignado de acuerdo a los perfiles establecidos.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 45 de 46

ARTÍCULO 89 CREACIÓN DE BITÁCORAS Y LOGS DE AUDITORÍA

El DTIC debe definir y crear los mecanismos para la creación de bitácoras y Logs que registren datos o información sobre quién, qué, cuándo, dónde y por qué ocurre un evento para una aplicación o para una base de datos, así como programar revisiones de controles de Seguridad de la Información incluyendo el análisis de vulnerabilidades.

 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL	POLITICAS DE SEGURIDAD INFORMÁTICA	Código: DGA-DTIC-001
		Fecha: 15/10/2015
		Versión: 3.0
		Página 46 de 46

9 REFERENCIAS BIBLIOGRÁFICAS

Manual de normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización. La Gaceta Nº 107 del 5 de junio, 2002.

ISO/IEC 27002:2008 Código de práctica para la gestión de Seguridad de la Información.

Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa.

http://portal.uned.es/portal/page?_pageid=93,1111671,93_20526767&_dad=portal&_schema=P
ORTAL

http://es.wikipedia.org/wiki/Base_de_datos

<http://lema.rae.es/drae/?val=Hardware%3A>

Definiciones redactadas por Funcionarios del DTIC.