Ministerio de Trabajo, Empleo y Seguridad Social

Subsecretaría de Coordinación

Dirección General de Informática e Innovación Tecnológica

Políticas de Seguridad de la Información

Autorizaciones		
Confecciona:	**Revisan:**	**Aprueba:**
Dirección General de Informática e innovación Tecnológica	Comité de Seguridad de la Información del MTEySS	Sr. Ministro

Contenido

1. Introducción

La información es un recurso sumamente valioso para el MTEySS. Puede existir en muchas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o medios electrónicos, presentada en imágenes, o expuesta en una conversación.

Cualquiera sea la forma adquirida, los medios por los cuales se distribuye o almacena, la información debe ser protegida en forma adecuada.

La Seguridad de la Información se logra implementando un conjunto adecuado de controles, abarcando *políticas, normas, procesos, procedimientos y documentos técnicos.*

Objetivos

Los objetivos de la implementación de Políticas de Seguridad de la Información en el MTEySS son los siguientes:

- protección de la información del MTEySS,
- gestión de riesgos de seguridad, adecuada al MTEySS,
- compromiso de mejora continua en la protección de los datos del MTEySS,
- establecimiento de políticas y de normas,
- comunicación, y concientización sobre los aspectos de Seguridad de la Información en forma pertinente, accesible y comprensible.
- establecimiento de un proceso eficiente de gestión de incidentes de seguridad.

Alcance

Las Políticas de Seguridad de la Información deben ser conocidas y cumplidas por:

- toda la planta de personal del MTEySS, funcionarios políticos, técnicos, contratados, sea cual fuere su nivel jerárquico y su situación de revista,
- organizaciones externas, contratistas y público en general-personas físicas o jurídicas- que accedan o hagan uso de la información ofrecida por el MTEySS,
- las instalaciones y los sistemas de información donde se almacenen, produzcan y/o procesen datos del MTEySS, bajo cualquier formato o metodología.

1.1 Aspectos y Riesgos en la gestión de Seguridad de la Información

Los siguientes aspectos son relevantes:

- la información es el activo más valioso del MTEySS,
- la seguridad absoluta no existe. Se trata de reducir el riesgo a niveles aceptables para la protección de la información del MTEySS,
- la seguridad no es un producto o un proyecto, sino que es una actividad continua,
- la gestión de seguridad requiere el soporte de todo el Organismo, a los fines de proteger con éxito la información,
- la seguridad debe integrarse tanto con los procesos relativos a la información y como los de gestión de la Organización.

Los riesgos que pueden impactar sobre la gestión de Seguridad de la Información son:

- temor ante el cambio de procesos y/o procedimientos: resistencia de las personas,
- discrepancias entre las áreas de toma de decisión,
- inadecuada delegación de responsabilidades en áreas técnicas, exclusivamente,
- falta de integración de la seguridad de la información a los procesos del MTEySS,

- implementación de medidas técnicas, sin los consiguientes procesos de concientización, gestión y organización,
- falta de comunicación.

1.2 Propiedad de los Recursos de Información del MTEySS

El MTEySS es propietario de los *recursos de información.*

Para cumplimentar su misión y objetivos, el Organismo pone a disposición de personas autorizadas, los recursos antes mencionados.

A los fines de la protección de sus datos, el MTEySS implementará procesos de auditoría de los recursos de información - p. ej.: mensajes de correo, archivos de usuarios, puestos de trabajo, etc.-, a fines de utilizarlos cuando las circunstancias lo exijan.

1.3 Accesos a la Información del MTEySS

Todo usuario que requiera el acceso a datos del Organismo deberá estar autorizado e identificado adecuadamente.

Para el caso de sistemas informáticos, el proceso de identificación se realiza mediante la llamada *cuenta de acceso,* Dicha cuenta deberá ser autenticada antes que se acceda al recurso.

1.4 Estructura documental de las Políticas de Seguridad de la Información del MTEySS

La presente versión de las políticas de Seguridad de la Información del MTEySS se basa en el Modelo aprobado por ONTI-ICIC, en octubre de 2013. Se mantienen los conceptos fundamentales allí expresados, así como la estructura de *cláusulas, políticas, categorías y controles,* adaptando los conceptos técnicos para su aplicación según las características propias del MTEySS.

2. Organización de la Política de Seguridad de la Información

Generalidades

Dado que los conceptos de las Políticas de Seguridad de la Información deben ser parte de la cultura organizacional, es necesario el compromiso manifiesto, tanto de las Autoridades Máximas, como de los Responsables Primarios de las diferentes áreas del MTEySS.

Objetivo

Se asignarán roles funcionales a todo nivel de la estructura jerárquica del Organismo, a los fines de la implementación y el cumplimiento de esta Política de Seguridad de la Información.

A los fines de proteger adecuadamente a los datos, sistemas y recursos de información del MTEySS, frente a amenazas, internas o externas, deliberadas o accidentales, se indicarán las responsabilidades en el cumplimiento de la seguridad, y la normativa legal vigente, desde la perspectiva de la confidencialidad, la integridad y la disponibilidad de la información,

Alcance

Las Políticas de Seguridad de la Información son de aplicación obligatoria para todo el personal del MTEySS, cualquiera sea su situación de revista, el área a la cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe.

Política

2.1 Categoría: Roles funcionales en la Política de Seguridad de la *información*

Objetivo

Proporcionar al MTEySS el marco de gestión para el tratamiento de la Seguridad de la Información, en concordancia con los requerimientos y las leyes y regulaciones relevantes.

2.1.1 Control: Definición de Roles

Los siguientes actores participan en la gestión de Seguridad de la información del MTEySS:

- Autoridad Máxima,
- Propietarios de la Información,
- Comité de Seguridad de la Información,
- Coordinador del Comité de Seguridad de la Información,
- Responsables de Recursos Humanos, Capacitación, Informática, Seguridad de la Información, Seguridad Física, Área Legal, Área Administrativa, Unidad de Auditoría Interna,
- Personal técnico,
- Usuarios.

2.1.1.1 Autoridad Máxima

Enfatiza la importancia de proteger la información del MTEySS y da su apoyo explícito a la formulación de Políticas de Seguridad de la Información para el Organismo, aprobando el documento que contiene dichas políticas, y sus actualizaciones.

Las funciones y responsabilidades relativas a las actividades de Autoridad Máxima sobre los aspectos de las Políticas de Seguridad de la Información quedan asignadas al Sr. Ministro de Trabajo, Empleo y Seguridad Social.

2.1.1.2 Propietarios de la Información

Los Propietarios de la Información, en adelante llamados *Responsables Primarios*, son aquellas Autoridades al frente de las distintas áreas ministeriales, con uso y manejo de la información que les sea pertinente.

Los Responsables Primarios deben dar soporte activo a la Seguridad de la Información, a través de una dirección clara, compromiso demostrado, y una adecuada delegación de las responsabilidades en la protección de los datos del MTEySS.

El Responsable Primario puede delegar la administración de las funciones de seguridad a personal idóneo en su cargo, conservando el compromiso de cumplimiento de las mismas.

La delegación de la administración por parte de los responsables primarios será documentada y proporcionada al Responsable de Informática.

2.1.1.3 Comité de Seguridad de la Información

El Comité de Seguridad de la Información se halla integrado por representantes de todas las áreas sustantivas del MTEySS. A través del mismo se establece el marco de gestión de la Seguridad de la Información dentro del Organismo.

Por *resolución MTEySS 54/06, se* creó el Comité de Seguridad de la Información, dentro del ámbito del Organismo, siendo sus funciones las estipuladas en la *Decisión Administrativa de Jefatura de Gabinete Nro 669/04-Art 4.*

2.1.1.4 Coordinador del Comité de Seguridad de la Información

El Comité de Seguridad debe contar con un Coordinador, a los fines de impulsar la implementación de las presentes Políticas y determinar las acciones a seguir.

El rol de Coordinador del Comité de Seguridad queda asignado al Sr. Subsecretario de Coordinación.

2.1.1.5 Responsable de Recursos Humanos

El rol relativo a la implementación de medidas de protección de los recursos humanos del MTEySS queda asignado al Director General de Gestión de Recursos Humanos.

2.1.1.6 Responsable de Capacitación

El rol relativo a las actividades de concientización sobre los aspectos de las Políticas de Seguridad de la Información queda asignado al Director de Capacitación y Desarrollo de Carrera.

2.1.1.7 Responsable de Informática

El rol relativo a la implementación y gestión sobre la infraestructura tecnológica, así como los aspectos de seguridad informática del MTEySS, queda asignado al Director General de Informática e Innovación Tecnológica.

2.1.1.8 Responsable de Seguridad de la Información

El rol relativo a la implementación y gestión de seguridad de la información del MTEySS queda asignado al Director General de Despacho, Mesa de Entradas y Archivo.

2.1.1.9 Responsable del Seguridad Física

El rol relativo a la implementación y gestión de medidas de protección física y ambiental sobre los recursos de información del MTEySS queda asignado al Director General de Administración.

2.1.1.10 Responsable del Área Legal

El rol relativo a la verificación del cumplimiento legal de las Políticas de Seguridad de la Información queda asignado al Director General de Asuntos Jurídicos.

2.1.1.11 Responsable del Área Administrativa

Las responsabilidades relativas a la verificación de los requisitos administrativos y contractuales relacionados con las Políticas de Seguridad de la Información quedan asignadas al Director General de Administración.

2.1.1.12 Responsable de la Unidad de Auditoría Interna

El Responsable de la Unidad de Auditoría Interna realizará revisiones independientes sobre la vigencia, implementación y gestión de las Políticas de Seguridad de la Información, a efectos de

garantizar que las prácticas del MTEySS reflejan adecuadamente lo dispuesto en este documento.

2.1.2 Control: Definición de Tipos de Usuarios

A los efectos del acceso y el uso de la información del MTEySS, se establecen los siguientes tipos de usuario:

- usuario interno,
- usuario de organizaciones externas,
- usuario contratista,
- usuario público.

2.1.2.1 Usuario Interno

Este usuario accede a datos y utiliza los recursos de información a través de la red interna de datos, o desde/hacia Intranet/Internet (p. ej.: vía redes privadas virtuales o correo electrónico en la Web).

Son usuarios internos los siguientes:

- Autoridades, funcionarios jerárquicos, agentes y empleados del MTEySS. Se incluye a todo aquel que se encuentre encuadrado bajo una modalidad de contratación, p. ej.: contratos bajo planta transitoria, o locación de servicios,
- técnicos, agentes y empleados que desarrollan, administran, procesan información, programan y/o dan soporte a recursos informáticos. Se los denomina *usuarios informáticos*.

2.1.2.2 Usuario de Organizaciones Externas

Tercera parte, no perteneciente al MTEySS. Posee acceso a datos o sistemas propiedad del MTEySS, según algún acuerdo especial con el Organismo. P. ej.: Conciliadores, Oficinas de Empleo, funcionarios de instituciones públicas o privadas.

Este tipo de usuario puede utilizar los recursos del MTEySS publicados en: la red de interna de datos, Intranet, Extranet o Internet.

2.1.2.3 Usuario contratista

Tercera parte, no perteneciente al MTEySS, vinculado a éste mediante un contrato para llevar a cabo un trabajo u obra determinada. P. ej.: proveedores de bienes servicios informáticos, consultoras.

2.1.2.4 Usuario Público

Población en general, que accede a datos o sistemas del MTEySS publicados en Extranet o Internet.

2.2 Categoría: Responsabilidades en la Política de Seguridad de la información

Objetivo

Definir claramente las responsabilidades en la implementación de las Políticas de Seguridad de la Información del MTEySS

2.2.1 Control: Asignación de Responsabilidades

2.2.1.1 Máxima Autoridad

La máxima autoridad del organismo, Sr. Ministro de Trabajo, Empleo y Seguridad Social de la Nación, aprueba esta Política, así como también debe revisar periódicamente los beneficios de la implementación de la misma.

2.2.1.2 Propietarios de la Información

Los Responsables Primarios deben:

- clasificar la información que se encuentra a su cargo, según un nivel de sensibilidad y criticidad, manteniendo actualizaciones periódicas de la misma,
- autorizar a los usuarios que requieran acceder a la información a su cargo, de acuerdo a funciones y competencia,
- identificar cómo manejar no-conformidades,
- colaborar y aprobar las metodologías y procesos para la seguridad de la información a su cargo (p. ej.: evaluación del riesgo a la información),
- documentar e informar formalmente sobre todos los incidentes que impacten sobre la Seguridad de la Información, dentro de su área de competencia,
- designar formalmente a aquellas personas que serán sus delegados, a los fines de las funciones indicadas en los párrafos anteriores.

2.2.1.3 Comité de Seguridad de la Información

El Comité de Seguridad deberá:

- definir y proponer a la máxima autoridad del MTEySS el documento de Políticas de Seguridad de la Información,
- generar y gestionar las revisiones y actualizaciones al documento de Políticas de Seguridad de la Información,
- verificar que se administren los riesgos que impacten sobre las políticas de seguridad y los recursos de información del Organismo,
- verificar el monitoreo y el tratamiento de incidentes relativos a la seguridad de la información, impulsando su resolución,
- aprobar las iniciativas que incrementen la seguridad de la información, de acuerdo con las responsabilidades y operatoria implementada por cada área,
- apoyar la implementación de controles específicos de seguridad de la información para los procesos del MTEySS,
- promover e implementar la difusión y apoyo a la Seguridad de la Información dentro del Organismo,
- verificar la existencia de mecanismos de continuidad de las operaciones, frente a interrupciones imprevistas,

2.2.1.4 Coordinador del Comité de Seguridad de la Información

El Coordinador del Comité de Seguridad de la Información impulsará la implementación de la presente Política.

2.2.1.5 Responsable de Recursos Humanos

El Responsable del área de Recursos Humanos deberá:

- comunicar la presente Política a todo el personal, así como de los cambios que en ella se produzcan,
- notificar a todo el personal las obligaciones y responsabilidades respecto del cumplimiento de la Políticas de Seguridad de la Información, las normas, procedimientos y prácticas que surjan de aquéllas, y lo relativo al uso, tratamiento y protección de la información del MTEySS,
- incluir las funciones relativas a la Seguridad de la Información en las descripciones de puesto del personal.

2.2.1.6 Responsable de Capacitación

Sus responsabilidades son:

- generar y coordinar tareas de capacitación continua y concientización, en materia de Seguridad de la Información, tanto a Responsables Primarios, usuarios internos, organizaciones externas y/o contratistas que accedan a datos del MTEySS.

2.2.1.7 Responsable de Informática

Sus responsabilidades son:

- implementar requerimientos y tareas relacionados con la operación, administración y soporte de los sistemas y recursos de tecnología y seguridad informática de propiedad del MTEySS, dentro del ámbito de su competencia,
- controlar el desarrollo y el soporte de los aplicativos, siguiendo una metodología apropiada de ciclo de vida, e incluyendo medidas de seguridad informática, en todas sus fases,
- implementar procedimientos de acceso a los recursos informáticos del Organismo, según los requerimientos formales elevados por los Responsables Primarios,
- implementar la aplicación de las medidas necesarias para la proteger la infraestructura donde reside la información del MTEySS,
- intervenir en la implementación de planes de continuidad de las actividades del MTEySS,
- definir y documentar normas y procesos claros y efectivos con respecto al uso de los recursos informáticos del MTEySS.

2.2.1.8 Responsable de Seguridad de la Información

Sus responsabilidades son:

- cubrir los requerimientos y tareas de Seguridad de la Información, dentro del ámbito de su competencia,
- investigar y verificar la implementación de mecanismos de seguridad informática en los sistemas de procesamiento de información,
- asesorar y asistir al personal del MTEySS, organizaciones externas y/o contratistas, en materia de seguridad de la información,
- coordinar la interacción con Organizaciones especializados, en materia de Seguridad de la Información,
- investigar y analizar riesgos de accesos a la información del Organismo, en conjunto con los Responsables Primarios, de Informática, de Seguridad Física y Área Legal, donde corresponda,
- investigar, proponer y verificar la aplicación de las medidas necesarias para la proteger la información del MTEySS,
- documentar, analizar y efectuar seguimiento de todos los incidentes de seguridad de la información que se hayan reportado,
- colaborar en tareas de capacitación y concientización relativas a la seguridad de la información,
- verificar que la metodología de desarrollo de los aplicativos informáticos incluya medidas de seguridad de la información en todas sus fases,
- investigar, proponer y verificar los planes de continuidad de las actividades del MTEySS,
- colaborar en la definición de medidas de seguridad física para el MTEySS,
- verificar que el acceso a los recursos de información del MTEySS se implemente según los requerimientos formales establecidos por los Responsables Primarios, en coordinación con

los Responsables Primarios, de Informática, de Seguridad Física y Área Legal, donde corresponda.

2.2.1.9 Responsable de Seguridad Física

El Responsable de Seguridad Física deberá:

- implementar los controles de acceso y seguridad física de las personas, en el ámbito del MTEySS,
- asegurar que los requerimientos ambientales contribuyan a que la información del MTEySS se procese en forma eficaz y segura, mediante los recursos utilizados. Esta tarea se realizará en conjunto con el Responsable de Informática, de Seguridad de la Información y de los Responsables de la Información, donde corresponda,
- implementar el mantenimiento de edificios, oficinas e instalaciones donde se procese y/o almacene información, cualquiera sea el medio utilizado. En las tareas participarán, además, los Responsables de Seguridad de la Información e Informática, así como los Responsables Primarios, cuando corresponda,
- documentar, analizar y efectuar seguimiento de todos los incidentes de seguridad física que se reporten,
- intervenir en la definición de planes de continuidad de las actividades del MTEySS.

2.2.1.10 Responsable del Área Legal

Sus responsabilidades son:

- asesorar sobre los aspectos legales atinentes a la protección de la información del Organismo,
- verificar el cumplimiento de las presentes políticas en la gestión de todo tipo de contrato, compromisos de confidencialidad o acuerdos con usuarios de los servicios de información.

2.2.1.11 Responsable del Área Administrativa

El Responsable del Área Administrativa deberá verificar que todo contrato suscripto considere, en forma obligatoria, el cumplimiento tanto de las Políticas de Seguridad de la Información, así como de las normas, procedimientos y prácticas relacionadas.

2.2.1.12 Unidad de Auditoría Interna

La Unidad de Auditoría Interna deberá:

- verificar el cumplimiento de las especificaciones y medidas de Seguridad de la Información establecidas por esta Política, además de las normas, procedimientos y prácticas que de ella surjan,
- verificar que estas revisiones incluyan evaluaciones de mejoras y cambios necesarios en el enfoque de la seguridad, y las políticas y objetivos de control de seguridad,
- practicar auditorías periódicas, e independientes, sobre los sistemas y actividades vinculadas con la tecnología y seguridad de la información.

2.2.1.13 Usuarios

Los usuarios deben conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

2.2.2 Control: Responsabilidades en el Acceso a Instalaciones de Procesamiento de Información

Los Responsables Primarios autorizarán formalmente al uso de los recursos de procesamiento de la información a su cargo.

Tratándose de procesamiento informático, los requisitos serán comunicados a los Responsables de Informática y de Seguridad de la información, a los fines que éste efectúe el diseño y la

implementación adecuada, que permitan el cumplimiento de las Políticas y requerimientos de seguridad pertinentes.

Las siguientes pautas deben ser consideradas para el proceso de autorización:

- verificar el cumplimiento de los procesos y procedimientos de autorización formales vigentes en la organización, con estricto cumplimiento de las políticas de seguridad pertinentes,
- que tanto los componentes y dispositivos electrónicos, como los programas y aplicativos tengan una completa compatibilidad entre sí, cuando se trate de procesamiento informático de los datos del MTEySS,

2.2.3 Control: Compromisos de confidencialidad

Se definirán, implementarán y revisarán regularmente compromisos de confidencialidad o de no divulgación, a los fines de la protección de la información del MTEySS. Asimismo, se deberá cumplir con toda legislación o normativa que alcance al Organismo en materia de confidencialidad de la información.

Los compromisos se implementarán:

- con el personal del Organismo, en sus distintos niveles y formas de contratación,
- con Organizaciones que accedan o hagan uso de los datos del Organismo,
- con contratistas, estableciendo delimitaciones relativas al objeto y requisitos de los contratos que se implementen.

2.3 Categoría: Gestión con Grupos o personas externas

Objetivo

Mantener la seguridad y los recursos de procesamiento, ante el uso, el acceso o el intercambio de datos propiedad del MTEySS con usuarios de Organizaciones externas y/o contratistas. A tales efectos, se definirán acuerdos, contratos o convenios de confidencialidad, donde corresponda.

2.3.1 Control: Contacto con otras organizaciones

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles, las siguientes organizaciones se hallan altamente especializadas en temas relativos a la seguridad de la información:

- Oficina Nacional de Tecnologías de Información (ONTI),
- Coordinación de Emergencias en Redes Teleinformáticas,
- Dirección Nacional de Protección de Datos Personales.

La divulgación de información del MTEySS a personas no autorizadas queda prohibida.

El intercambio de información confidencial o sensible, a los fines de asesoramiento o de transmisión de experiencias, sólo se permitirá luego de haber implementado un Convenio de Confidencialidad previo.

2.3.2 Control: Coordinación del Contacto con otras organizaciones

Los Responsables de Seguridad de la Información y de Informática coordinarán el intercambio de conocimientos y las experiencias disponibles en el MTEySS, obteniendo asimismo asesoramiento de otros grupos de interés especial.

Las siguientes son consideraciones a tener en cuenta en el contacto con otros organizaciones:

- asegurar que el MTEySS se mantenga actualizado sobre nuevos conocimientos, prácticas y tendencias en materia de seguridad de la información,

- asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa,
- recibir alertas tempranas, avisos y recomendaciones ante ataques y vulnerabilidades,
- disponer de vínculos adecuados para el tratamiento de los incidentes de seguridad de la información.

2.3.3 Control: Aspectos relacionados con grupos externos

Ante la necesidad de otorgar acceso a la información a usuarios de organizaciones externas y/o contratistas, los Responsables de Informática, Seguridad de la Información y el Responsable Primario a cargo de los datos, efectuarán una evaluación de riesgos, a los fines de identificar los requerimientos de control específicos.

Se tendrán en cuenta los siguientes aspectos:

- los medios de procesamiento de información a los cuales necesita tener acceso los usuarios de organizaciones externas y/o contratistas,
- el tipo de acceso requerido (físico/lógico/remoto y a qué recurso),
- el tipo de recurso utilizado para acceder (dispositivo móvil, puesto de trabajo, recurso personal),
- la ubicación de la información (p.ej.: red interna, nube de datos),
- los motivos para los cuales se solicita el acceso,
- el valor de la información,
- los controles empleados por los usuarios de organizaciones externas y/o contratistas,
- diferentes medios y controles empleados por los usuarios externos y/o contratistas, cuando éstos almacenan, procesan, comunican, comparten e intercambian información del MTEySS,
- otorgamiento de los mínimos permisos necesarios,
- requisitos legales y normativos,
- la incidencia de este acceso en la seguridad de la información del MTEySS.

2.3.3.1 Organizaciones Externas

Se trata de Organizaciones que hacen uso de la información del MTEySS. Entre ellos, se encuentran:

- Oficinas de Empleo,
- consultorías externas de sistemas, proveedores de paquetes de sistemas,
- otras Organizaciones gubernamentales,
- accesos especiales (p. ej.: conciliadores laborales, abogados, inspectores, etc.),

2.3.3.2 Contratistas

Se trata de proveedores que, en virtud de especificaciones contractuales, pueden requerir un acceso a la información del MTEySS. Entre ellos, se encuentran:

- consultorías de auditoría externa,
- limpieza, "catering", guardia de seguridad y otros servicios de mantenimiento tercerizados,
- proveedores de servicios o de instalaciones especiales,
- pasantías y otras designaciones de corto plazo,
- servicios de soporte de hardware en garantía.

2.3.3.3 Requerimientos de Seguridad en los Contratos y Acuerdos con Organizaciones Externas, Contratistas y Público en general

El acceso a la información del MTEySS de las organizaciones externas, contratistas y público en general debe basarse en contratos y/o acuerdos formales, que consideren los requerimientos de seguridad establecidos en estas Políticas.

Los acuerdos y/o contratos deberán indicar la aplicación de los siguientes controles:

- compromisos de confidencialidad, protección de activos y controles de accesos, que contemplen:
  - información, software y/o sistema al que se accederá,
  - responsabilidades y garantías para evitar fallas de seguridad, pérdida, modificación no autorizada o destrucción de datos y activos,
  - recuperación y/o destrucción de información y activos, en un momento convenido durante la vigencia del contrato,
  - identificación de quienes harán uso de la información,
  - integridad y disponibilidad,
  - restricciones a la copia y divulgación de información,
  - niveles de servicio esperados y aceptables,
  - obligaciones de las partes en el acceso a la información del MTEySS por parte de las organizaciones y contratistas
  - obligaciones en la cesión de datos a organizaciones externas o contratistas, si corresponde,
  - responsabilidades legales, por ej., sobre protección de datos y delitos informáticos,
  - derechos de propiedad intelectual, y protección de la información,
  - períodos de vigencia del compromiso de confidencialidad,
  - medios de almacenamiento/transferencia/acceso para la información,
  - métodos, procesos y procedimientos de acceso autorizados,
  - control y uso de identificadores únicos, p. ej.: IDs y contraseñas de usuarios,
  - procedimientos de autorización de acceso y privilegios de usuarios,
  - listas y/o perfiles de usuarios autorizados para utilizar los servicios ofrecidos,
  - derechos de uso de los servicios, tanto sobre la red interna o hacia Internet,
  - definición de criterios de desempeño comprobables,
  - elaboración y presentación de informes de desempeño por parte de los contratistas,
  - elaboración y presentación de informes de notificación e investigación de incidentes y violaciones a la seguridad.
- derecho del MTEySS a auditar, monitorear, revocar o restringir la actividad de las organizaciones externas y/o contratistas, tomando en cuenta:
  - la verificación de las responsabilidades contractuales,
  - la contratación de otra tercera parte para la realización de auditorías sobre las actividades realizadas,
- implementación de procedimientos para la resolución de problemas y contingencias,
- responsabilidades relativas a la instalación y soporte de hardware y software sea éste de propiedad del MTEySS o de las organizaciones externas o contratistas,

- controles y procedimientos para el acceso a aplicativos publicados en Internet, o en nubes de almacenamiento y/o procesamiento de datos del MTEySS,
- procesos claros y detallados sobre la gestión de cambios,
- controles de protección física requeridos y mecanismos que aseguren la implementación de los mismos, tano para equipamiento propio como para el ajeno, cuando corresponda,
- métodos y procedimientos de capacitación de usuarios y administradores de servicios y seguridad,
- controles que garanticen la protección contra software malicioso,
- la relación entre el MTEySS y los contratistas.

2.4 Categoría: Utilización de Recursos Informáticos Personales

Objetivo

Los recursos personales de los usuarios representan una potencial amenaza para la información del MTEySS, configurando además una posible exposición de la Organización al incumplimiento de las leyes vigentes.

La utilización de los recursos informáticos personales en el ámbito de la infraestructura de información del Organismo debe estar restringida. La excepción a esta política deberá ser evaluada por el Responsable de Seguridad de la Información, siendo autorizada tanto por el Responsable Primario del sector correspondiente como por el Responsable de Informática.

Los Responsables de Informática y Seguridad Física determinarán los requerimientos para que los recursos personales tengan el acceso lógico y físico al MTEySS, cuando corresponda.

Se implementarán procedimientos para la evaluación, registración y autorización de uso en el ámbito del MTEySS.

2.4.1 Control: Requerimientos de Seguridad en el empleo de Equipos Personales

Se tomarán en cuenta los siguientes puntos de control:

- tipo de recurso del MTEySS al que se accederá,
- uso que se le dará al recurso personal, dentro de la infraestructura del MTEySS,
- período de uso del recurso, dentro de la infraestructura del MTEySS,
- compatibilidad con la infraestructura tecnológica existente,
- responsabilidad del usuario dueño del recurso personal,
- condiciones de acceso a la red del MTEySS,
- términos de soporte de los recursos informáticos personales,
- requerimientos de las políticas de Seguridad de la Información del MTEySS,
- configuración de conexión a la red de datos,
- riesgos de daños sobre la información del Organismo,
- sistema operativo instalado, con las últimas actualizaciones de seguridad informática,
- instalación de un antivirus autorizado por el Organismo, con las últimas actualizaciones de seguridad informática,
- software instalado en el equipo personal. Su uso deberá ser evaluado por el responsable de Seguridad de la Información, siendo autorizado tanto por el Responsable Primario como por el Responsable de Informática,
- el software instalado no deberá ofrecer ningún riesgo de compromiso a la seguridad de la red de datos,

- condiciones ambientales donde se instalará el equipo personal,
- prohibición de uso o transferencia de la información personal residente en el recurso, dentro del ámbito del MTEySS,
- derecho del MTEySS a auditar, monitorear, y revocar o impedir la actividad en la red de datos. Se dará máxima prioridad a todos los casos donde haya riesgo a la seguridad de los datos del Organismo, así como al cumplimiento de las leyes vigentes,
- controles de protección física requeridos y mecanismos que aseguren la implementación de los mismos,
- controles que garanticen la protección contra software malicioso.

3. Evaluación y tratamiento de riesgos

Generalidades

Dado que no existe la seguridad completa, se debe conocer cuál es el conjunto de riesgos a los que se expone el MTEySS, a fin de tomar acciones para proteger la información. La gestión de riesgos, por ende, es pilar fundamental para la gestión de seguridad.

Objetivo

Conocer los riesgos a los que se expone el MTEySS en materia de seguridad de la información, a fin de dar apoyo a la toma de decisiones en materia de incidentes y controles de seguridad.

Alcance

Esta Política se aplica a toda la información procesada y administrada por el MTEySS, cualquiera sea el soporte en que se encuentre.

Responsabilidad

El Comité de Seguridad de la Información estará informado de los riesgos de seguridad de la información, apoyando el desarrollo y la vigencia del proceso de gestión de riesgos.

El Responsable de Seguridad de la Información, el Responsable de Informática y los Responsables Primarios, donde corresponda, definirán los procesos de gestión de riesgos de seguridad de la información.

Política

3.1 Categoría: Evaluación de los riesgos de seguridad

El MTEySS identificará y evaluará los riesgos a la información, efectuando una priorización de acuerdo a la relevancia de los bienes, y los objetivos de control aplicables. Los resultados permitirán determinar las acciones y las prioridades de tratamiento de los riesgos. A continuación, se implementarán los controles que se hayan seleccionado.

La evaluación de riesgos debe ser periódica, para estar en línea con los cambios organizacionales y los requerimientos de seguridad, por ejemplo: evolución de amenazas, nuevas vulnerabilidades, impacto de los incidentes, implementación de nuevos proyectos, etc.

La evaluación de riesgos debe efectuarse de manera metódica, a fin de brindar resultados comparables y reproducibles.

Una evaluación de riesgos puede alcanzar a todo el MTEySS, a una parte, a un sistema de información particular, o componentes específicos de un sistema o un servicio.

3.2 Categoría: Tratamiento de riesgos de seguridad

Una vez identificados los riesgos, se determinarán las políticas de tratamiento, de forma de llevar los riesgos a un nivel tolerable, implementando controles apropiados,

La implementación de controles de mitigación deberá tener en cuenta lo siguiente:

- requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales,
- objetivos organizacionales,
- requerimientos y restricciones operativos,
- costos de implementación y operación, en relación directa con la reducción de riesgos calculada.
- evaluación permanente de los controles implementados, para poder mejorar su eficiencia y su efectividad.

4. Cláusula: Gestión de Activos

Generalidades

El MTEySS debe tener un conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Los activos o bienes utilizados para procesar información del MTEySS deberán estar inventariados y clasificados según niveles de confidencialidad, sensibilidad, disponibilidad, integridad y criticidad, e integridad. Se tendrá en cuenta, además, la funcionalidad que cumplen los datos procesados, a los fines de asegurar una adecuada protección.

Se tendrá en cuenta la variación de la clasificación de un ítem de información, sea por efecto de una política predeterminada, porque la información se hace pública o porque es obsoleta.

Se definirán los niveles de clasificación, adecuados a la eficiencia, la eficacia y la funcionalidad de los controles y la gestión en general.

Cuando la información pase a ser obsoleta, se definirán procedimientos de eliminación, asegurando en todo momento los requerimientos de confidencialidad adecuados.

Objetivo

Son objetivos de la gestión de activos:

- garantizar que los activos de información reciban un apropiado nivel de protección,
- clasificar la información, registrando adecuadamente los niveles de confidencialidad, sensibilidad, integridad, disponibilidad y criticidad que correspondan a cada caso,
- definir niveles de protección y medidas de tratamiento especial acordes a la clasificación definida.

Alcance

Esta Política se aplica a toda la información propiedad del MTEySS, o que se halle administrada por éste, cualquiera sea el soporte en que ésta se encuentre y el medio utilizado para su acceso.

Asimismo, quedan alcanzados todos los usuarios que utilicen la información del Organismo.

Responsabilidad

Los Responsables Primarios deben establecer los criterios de clasificación a su cargo, en coordinación con los Responsables de Informática, de Seguridad de la Información, Seguridad Física y Administración, donde corresponda.

4.1 Categoría: Responsabilidad sobre los activos

Objetivo

Definir las funciones que impactan sobre la clasificación de los activos de información.

Política

4.1.1 Control: Inventario de activos

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable Primario, con la colaboración de los Responsables de Informática, Seguridad de la Información, Seguridad Física, Administración y Unidad de Auditoría, donde corresponda.

Los activos deben estar identificados e inventariados, considerando las siguientes pautas:

- el inventario debe actualizarse ante cualquier modificación de la información registrada,
- el inventario se revisará con una frecuencia mínima de 6 (seis) meses.

4.1.2 Control: Gestiones sobre los activos

Los activos de información son propiedad del Responsable Primario, a quien se asignan los recursos y datos relacionados con las funciones inherentes a las áreas a su cargo.

4.1.2.1 Definición de los activos de información del MTEySS

Los siguientes son activos de información:

- *documentos*: documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, contenido de sitios Web del Organismo. Los mismos pueden hallarse en soporte papel o en medios informáticos,
- *recursos de software*: aplicaciones, sistemas operativos, bases de datos y archivos, herramientas de desarrollo, utilitarios, aplicativos, plataformas de gestión y control,
- *activos físicos*: equipamiento informático (computadoras portátiles, impresoras, módems, puestos de trabajo, PCs, servidores, notebooks, netbooks, tablets, teléfonos inteligentes), dispositivos de comunicaciones (routers, switches, PABXs, máquinas de fax, contestadores automáticos, dispositivos wireless), medios magnéticos (cintas, discos), medios y dispositivos de almacenamiento portátiles (pen drives, etc), sistemas de registro gráfico y sonoro (cámaras fotográficas, filmadoras, sistemas de sonido, etc.),
- *servicios de TICs*: comunicaciones Web, Extranet e Intranet, servicios de conexión a nubes,
- *activos virtuales*: información almacenada o procesada en instalaciones de nube (cloud computing),
- *activos intangibles*: imagen del Organismo, reputación, habilidades y experiencia de las personas,
- *instalaciones físicas*: suministro eléctrico a centros de procesamiento, unidades de aire acondicionado, mobiliario, lugares de emplazamiento, sistemas de protección física, controles de acceso físico, etc.

4.1.2.2 Responsabilidades sobre los activos

Las funciones de propietario de la información y los activos que le caben al Responsable Primario, en lo atinente a seguridad de la información, son:

- establecer los requisitos de seguridad de los activos,
- clasificar los activos en función a la sensibilidad, la criticidad, la confidencialidad, la disponibilidad y la integridad, con la colaboración de los Responsables de Informática, Seguridad de la Información, Administración y/o Seguridad Física, donde corresponda,
- informar sobre cualquier cambio que afecte a la clasificación de los activos a los Responsables de Informática, Seguridad de la Información, Administración y/o Seguridad Física, donde corresponda,
- verificar la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

El Responsable de Informática debe proponer e implementar la infraestructura tecnológica, los sistemas de procesamiento, los accesos y los controles de seguridad informática.

El Responsable de Seguridad de la Información debe proponer y verificar los mecanismos de acceso a la información, garantizando que los niveles de clasificación sean estrictamente observados.

El Responsable de Seguridad Física establecerá e implementará los controles adecuados para el acceso físico a los activos, donde corresponda.

4.1.2.3 Delegación de Responsabilidades sobre los activos

Los Responsables Primarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservando, no obstante, la responsabilidad por el cumplimiento de las mismas.

La delegación de la administración será documentada proporcionada a los Responsables de Informática, Seguridad de la Información, Administración y/o Seguridad Física, donde corresponda.

4.1.3 Control: Uso aceptable de la información y los activos

Se establecerán, documentarán e implementarán reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento.

Los Responsables de Informática, Seguridad de la Información, Administración y Seguridad Física, donde corresponda, establecerán procesos de verificación del uso adecuado de los activos.

Los Responsables Primarios deberán ser informados de aquellos casos donde se efectúe una violación a dichas reglas, a fin de tomar las medidas pertinentes.

4.2 Categoría: Clasificación de la información

Objetivos

Establecer una clasificación de criticidad de la información del MTEySS, así como los activos que la procesan, de manera que se implementen protecciones adecuadas.

Asegurar que los controles de seguridad física, informática u otros sean los correspondientes al nivel de clasificación establecido.

Definir un conjunto apropiado de niveles de clasificación, y que los mismos sean fehacientemente comunicados a las partes pertinentes en la gestión de operación, soporte y seguridad.

4.2.1 Control: Criterios de clasificación

Para clasificar un activo de Información, se evaluarán las tres características básicas de la seguridad: confidencialidad, integridad y disponibilidad. En función de ellas, el Responsable Primario establecerá el criterio de criticidad que se aplicará a cada activo.

4.2.1.1 Confidencialidad

Nivel 0- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del MTEySS o no. USO PÚBLICO,

Nivel 1- Información que puede ser conocida y utilizada por todos los empleados del MTEySS y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el MTEySS, el Sector Público Nacional o terceros. USO RESERVADO - INTERNO,

Nivel 2- Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al MTEySS, al Sector Público Nacional o a terceros. USO RESERVADO – CONFIDENCIAL,

Nivel 3- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del MTEySS, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. USO RESERVADO – SECRETA.

4.2.1.2. Integridad

Nivel 0 - Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del MTEySS,

Nivel 1 - Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el MTEySS, el Sector Público Nacional o terceros,

Nivel 2 - Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el MTEySS, el Sector Público Nacional o terceros,

Nivel 3 - Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al MTEySS, al Sector Público Nacional o a terceros.

4.2.1.3. Disponibilidad

Los criterios indicados serán tenidos en cuenta por los Responsables Primarios, para establecer los siguientes niveles de disponibilidad: No Clasificado, Bajo, Medio, Alto, Muy Alto y Crítico.

Nivel 0 - Información cuya inaccesibilidad no afecta la operatoria del Organismo,

Nivel 1 - Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el MTEySS, el Sector Público Nacional o terceros,

Nivel 2 - Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas al MTEySS, al Sector Público Nacional o a terceros,

Nivel 3 - Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas al MTEySS, al Sector Público Nacional o a terceros.

En este criterio, y a afecto de evaluar las pérdidas, debe considerarse también si:

- los datos son generados en el MTEySS o por organizaciones externas,
- los plazos de gestión son establecidos por organizaciones externas,
- las gestiones con la información incluyen presencia del público,
- las gestiones con la información son realizadas mediante acceso desde Internet.

4.2.1.4. Criticidad

Al considerar las pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Finalmente, el nivel de criticidad se basará en las características indicadas en los Puntos *7.2.1.1* a *7.2.1.3*, determinándose la siguiente clasificación:

Criticidad Baja - la información es Pública, con Integridad No Clasificada o Baja y Disponibilidad No Clasificada.

Criticidad Media - la información es Reservada de Uso Interno, Integridad y Disponibilidad nivel medio.

Criticidad Alta - la información es Reservada-Confidencial, requiere Integridad Alta y Disponibilidad Alta, Muy Alta o Crítica.

4.2.1.5. Gestión de Clasificación de la Información

El Responsable Primario, con la colaboración de las áreas de Informática, Seguridad de la Información, Seguridad Física y/o Administración, donde corresponda, identificará los recursos a su cargo y les asignará el nivel de clasificación que corresponda.

4.2.1.6 Pautas adicionales para clasificar la Información

Se establecerán:

- perfiles funcionales, de operación y acceso para los usuarios que se requieran,
- fechas de efectividad y/o caducidad del nivel de clasificación,
- procedimientos de asignación/modificación de niveles,
- procedimientos de autorizaciones y comunicación.

4.2.1.7 Modificación del nivel de clasificación

Cuando se lo requiera, el nivel de clasificación de la información será modificado por el Responsable Primario, con la colaboración de los Responsables de Informática, Seguridad de la Información, Administración y/o Seguridad Física, donde corresponda.

4.2.2 Control: Rotulado y manejo de la información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido.

Se contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- copia a cualquier medio de almacenamiento autorizado,
- manipulación de datos por medio de aplicaciones y/o sistemas informáticos,
- manipulación y almacenamiento de datos en papel,
- manipulación y almacenamiento de datos en dispositivos móviles,
- almacenamiento para resguardo o recupero,
- transmisión por correo, fax, correo electrónico,
- guarda de medios de almacenamiento,
- transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.),
- manipulación y/o procesamiento de datos en redes externas (*cloud computing*),
- publicación masiva o restringida en algún medio gráfico, Internet o Intranet.

Los niveles de clasificación, deben contemplar procedimientos de manejo seguro, incluyendo las actividades de procesamiento, almacenaje, transmisión, desclasificación y destrucción.

5. Cláusula: Recursos Humanos

Generalidades

Los recursos humanos son un factor primordial en los procesos de gestión de la seguridad de la información del MTEySS.

La protección del personal del Organismo es prioritaria, así como la necesidad de reducir riesgos por error humano en la manipulación de la información, comisión de ilícitos contra el MTEySS, o uso inadecuado de las instalaciones.

Es fundamental, asimismo, la capacitación continua al personal, sobre las medidas de seguridad que afectan al desarrollo de sus funciones, y lo atinente a mantener la debida confidencialidad.

En lo referente al cese de la relación con el Organismo, debe evitarse el posible compromiso sobre la información mientras dura el proceso de desvinculación.

Asimismo, deben establecerse las sanciones a aplicar en caso incumplimiento de las políticas de seguridad.

Objetivo

Los objetivos de esta cláusula son:

- explicitar las responsabilidades sobre la seguridad, tanto en la etapa de ingreso y/o reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado,
- incluir en la gestión de los recursos humanos aquellos aspectos que contribuyan a mitigar riesgos por error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y/o manejo no autorizado de la información,
- garantizar que los usuarios estén al tanto de las amenazas, vulnerabilidades y aspectos clave en materia de seguridad de la información, de forma que se encuentren capacitados para respaldar la Política de Seguridad del MTEySS en el transcurso de sus tareas normales,
- definir e implementar Compromisos de Confidencialidad y de Uso Adecuado de los Recursos de Información, con todo el personal y usuarios externos que se desempeñen en el ámbito del Organismo,
- establecer los mecanismos para que los procesos de desvinculación del Organismo contemplen la protección de la información,
- definir sanciones para el caso que se violen las políticas de seguridad.

Alcance

Esta Política se aplica a todo el personal del MTEySS, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito del Organismo.

Responsabilidad

El Responsable del Recursos Humanos deberá:

- incluir las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados,
- informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información,
- gestionar los Compromisos de Confidencialidad con el personal ,
- coordinar las tareas de capacitación de usuarios respecto de la presente Política,

El Responsable del Área Legal deberá:

- colaborar en la confección de los Compromisos de Confidencialidad,
- asesorar sobre las sanciones a ser aplicadas por incumplimiento de la presente Política,
- tratar los incidentes de seguridad que requieran de su intervención.

El Responsable de Seguridad de la Información colaborará en la formulación de contenidos para los planes de concientización y/o capacitación en materia de seguridad de la información.

El Responsable de Seguridad Física colaborará en la capacitación sobre los procedimientos que hagan a la seguridad física del personal y terceros que se desempeñen en el ámbito del MTEySS.

Política

5.1 Categoría: Antes del empleo

Objetivo

Asegurar que las responsabilidades de seguridad sean conocidas en la etapa de contratación del personal, en los términos y condiciones del empleo y en las adecuadas definiciones del puesto a cubrir.

Asimismo, se debe garantizar que los candidatos entiendan sus futuras responsabilidades, y sean idóneos para los roles para los cuales son considerados.

5.1.1 Control: Obligaciones con respecto a la Seguridad de la Información

Se definirán las obligaciones en materia de seguridad, las que serán incorporadas en la descripción de responsabilidades de los puestos de trabajo.

Se deberán considerar lo siguiente:

- responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad,
- responsabilidades específicas vinculadas a la protección de cada uno de los activos, la ejecución de procesos o actividades de seguridad determinadas.

Los roles y obligaciones serán comunicados a los candidatos para el puesto de trabajo durante el proceso de preselección.

5.1.2 Control: Investigación de antecedentes

Cuando se inician las gestiones de búsqueda de personal, se llevarán a cabo controles de verificación. Estos controles incluirán todos los aspectos que indiquen las normas que, a tal efecto, alcanzan al MTEySS.

Las verificaciones deben incluir:

- acreditación fehaciente de la identidad del candidato,
- currículum vitae del postulante,
- referencias satisfactorias,
- confirmación de títulos académicos y profesionales mencionados por el postulante.

5.1.3 Control: Términos y condiciones de empleo

Los términos y condiciones de empleo deberán contemplar derechos y obligaciones del empleado, relativos a las leyes de Propiedad Intelectual y/o la legislación de protección de datos personales y de delitos informáticos.

5.2 Categoría: Durante el empleo

Objetivo