- definir los procedimientos para:
  - el control de cambios a los sistemas,
  - la verificación de la seguridad de los entornos, plataformas y bases de datos que interactúan con los sistemas,
  - el control sobre código malicioso,
  - la definición de las funciones del personal involucrado en el proceso de entrada de datos, con el Responsable de Informática y el Responsable Primario, donde corresponda,
- definir los procedimientos de administración de claves,

El Responsable de Informática tendrá las siguientes responsabilidades:

- proponer la asignación de funciones de implementador y de testeador al personal de su área que considere adecuado. Dichas funciones se hallan especificadas en el *Capítulo 7.1.4 Control: Separación entre las Instalaciones de Desarrollo, Prueba, Homologación y Producción*),
- verificar el cumplimiento de los controles y las medidas de seguridad a ser incorporadas a los sistemas,
- proponer quiénes realizarán la administración de las técnicas criptográficas y las claves.

El Responsable del Área Administrativa, con la participación del Responsable del Área Legal, incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los acuerdos y contratos por el desarrollo de software con organizaciones externas y/o contratistas.

Política

9.1 Categoría: Requerimientos de Seguridad de los Sistemas

Objetivo

Los procesos operativos del MTEySS se apoyan en una infraestructura tecnológica y de comunicaciones, dando soporte a sistemas y aplicaciones informáticas propietarias y a paquetes de software adquiridos. Se debe garantizar que la seguridad sea una parte integral de los elementos descriptos.

9.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad

Los sistemas informáticos propios y de terceros, así como las mejoras o actualizaciones de los mismos, deben incorporar controles de seguridad en la etapa de definición de especificaciones.

En esta tarea deben participar los Responsables Primarios, de Informática, de Seguridad de la Información y la Unidad de Auditoría Interna. Se podrá recurrir a certificaciones y evaluaciones independientes para los productos a utilizar, en caso de ser necesario.

Se deben tener en cuenta las siguientes consideraciones:

- *definición de requerimientos.* Los requerimientos del sistema se definirán en las etapas de análisis y diseño. Mediante un proceso de evaluación de riesgos, se identificarán los controles y especificaciones de seguridad a incorporar,
- *controles automáticos y manuales.* Se propenderá a la utilización de controles automáticos, permitiéndose controles manuales como excepción,
- *relación de los requerimientos y controles con respecto al bien a proteger.* Los requerimientos y controles de seguridad definidos deben ser proporcionales al valor del activo que se quiere proteger y al riesgo que pueden correr las actividades del MTEySS,

- *incorporación temprana de controles.* Se debe considerar que los controles introducidos en la etapa de diseño, tienen un costo de implementación y mantenimiento significativamente menor que aquellos incluidos durante o después de la instalación.

9.2 Categoría: Seguridad en los Sistemas de Aplicación

Objetivo

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

- la validación efectiva de datos de entrada,
- el procesamiento interno,
- las interfaces de los sistemas y la autenticación de mensajes entre los mismos,
- la validación de datos de salida,
- la revisiones de accesos, indicando quién lo realiza, en qué forma, con qué método y privilegios, a quiénes se informa el resultado,
- las alternativas a seguir frente a errores de validación en un aplicativo.

9.2.1 Control: Validación de Datos de Entrada

Los controles definidos en la etapa de diseño deberán asegurar la validez de los datos ingresados, y estarán ubicados tan cerca del punto de origen como sea posible. Se deberán verificar, asimismo, datos permanentes y tablas de parámetros.

9.2.1.1 Procedimientos de control de datos de entrada

Este procedimiento considerará los siguientes controles:

- validación de tipos de datos y caracteres ingresados,
- control de secuencia,
- control de entradas centralizado, inhibiendo las existencia de puertas traseras (backdoors),
- control de monto límite por operación y tipo de usuario,
- control del rango de valores posibles y su validez, según criterios predeterminados,
- control de paridad,
- control contra valores cargados en las tablas de datos.

Por otra parte, se llevará a cabo lo siguiente:

- definir responsabilidades, controles y funcionalidades para el personal involucrado en los procesos de entrada y modificación de datos,
- establecer controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo, y viceversa,
- establecer controles para evitar accesos por rutas alternativas o en forma directa, especialmente en aplicaciones en plataformas de Internet,
- para aplicaciones en plataformas de Internet, establecer procedimientos para que la validación de los datos ingresados se haga desde el lado del servidor,
- establecer revisiones periódicas de contenidos de campos clave y/o archivos de datos, determinando quién lo realizará, en qué forma, con qué método, quiénes deben ser informados del resultado, etc.

9.2.2 Control: Controles de Procesamiento Interno

En la etapa de diseño se deberán incorporar controles de validación, con el fin de minimizar los riesgos de fallas de procesamiento y/o en el manejo de errores.

Para ello se implementarán:

- controles de validación de los datos generados por el sistema,
- identificación de funciones de modificación, agregado y/o eliminación de datos,
- integridad de datos y del software, funcionalidades de corrección de datos por parte de los usuarios,
- verificaciones de ejecución de los aplicativos en el momento adecuado, previniendo el procesamiento fuera de secuencia,
- control de la integridad de registros y archivos.
- detención y reanudación del procesamiento ante una falla,
- generación de alertas para detectar cualquier anomalía en la ejecución de las transacciones,
- revisión periódica de los registros de auditoría.
- procedimientos de finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

9.2.3 Control: Autenticación de Mensajes

9.2.3.1 Transmisión de mensajes entre programas

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto "*9.3 Categoría: Controles Criptográficos*".

9.2.3.2 Interfaces entre sistemas

Se deberán establecer controles comunes en los sistemas que estén interconectados, tales como:

- verificaciones ante fallas de procesamiento en un sistema, estableciendo rutinas de contingencia en los aplicativos interconectados al mismo,
- rótulos en las interfaces, de manera que se identifique claramente los sistemas que se hallan interconectados,
- verificación de integridad de los datos y del software cargado o descargado entre computadoras.

9.2.4 Control: Validación de Datos de Salida

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

- validez de los datos presentados,
- conciliación de cuentas para asegurar el procesamiento de todos los datos,
- determinación del grado de exactitud, totalidad, precisión y clasificación de los datos presentados ante las salidas o los sistemas conectados,
- definición de responsabilidades y controles sobre el personal afectado al proceso de salida de datos.

9.2.5 Control: Mensajes de Error

Los mensajes de error deben manejarse en forma centralizada, dentro del contexto de la aplicación. Los errores de sistemas no deben llegar de ninguna manera al usuario en forma directa.

Los avisos de error serán interceptados por el aplicativo y se los reemplazará por comentarios simples, adaptados al usuario final. El contenido de dichos avisos sólo debe ser de carácter orientativo, proporcionando la menor información posible.

Por otra parte, para tareas de mantenimiento y/o depuración del sistema, se emitirán mensajes de error con el mayor detalle posible, y se almacenarán en un registro exclusivo, para acceso del personal técnico que corresponda.

9.3 Categoría: Controles Criptográficos

Objetivo

Se utilizarán sistemas y técnicas criptográficas para la protección de la información con el fin de asegurar un adecuado nivel de confidencialidad, integridad, autenticación y/o no repudio, según surja del resultado de un análisis de riesgos.

Se debe desarrollar una política sobre el uso de controles criptográficos. Se debe establecer una gestión clave para sostener el uso de técnicas criptográficas.

9.3.1 Control: Política de Utilización de Controles Criptográficos

El MTEySS incorpora una política de utilización de controles criptográficos.

La determinación de los casos de utilización, así como los procedimientos correspondientes, surgirá como resultado de una evaluación de riesgos efectuada por el Responsable de Informática y el Responsable de Seguridad de la Información, junto con los Responsables Primarios.

9.3.1.1 Utilización y procedimientos

Se tomará en cuenta lo siguiente:

- uso de controles criptográficos en los siguientes casos:
  - para la protección de claves de acceso a sistemas, datos y servicios,
  - para transmitir información clasificada, fuera del ámbito del MTEySS,
  - para resguardo de información, cuando corresponda,
  - como requerimiento para casos de aplicación de firma digital.
- desarrollo de procedimientos respecto de:
  - la administración de claves,
  - la recuperación de información cifrada en caso de pérdida,
  - compromiso o daño de las claves,
  - reemplazo de las claves de cifrado.

9.3.1.2 Algoritmos de Cifrado y Tamaños de Clave

Se presenta a continuación un listado de los algoritmos y longitudes de clave considerados seguros a la fecha. Se recomienda verificar esta condición periódicamente, a fin de poder efectuar las actualizaciones que correspondan.

1. Cifrado Simétrico	
Algoritmo	**Longitud de Clave en Bits**
AES	128/192/256

3DES	168
IDEA	128
RC4	128
RC2	128

2. Cifrado Asimétrico		
Casos de Utilización	**Algoritmo**	**Longitud de Clave en Bits**
Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048
	DSA	2048
	ECDSA	210
Para certificados de sitio seguro	RSA	1024
Para certificados de Certificador o de información de estado de certificados	RSA	2048
	DSA	2048
	ECDSA	210
Para certificados de usuario (personas físicas o jurídicas)	RSA	1024
	DSA	1024
Para digesto seguro	ECDSA	160
	SHA-1	256

9.3.2 Control: Cifrado

Según una evaluación de riesgos efectuada por los Responsables de Informática y de Seguridad de la Información, junto con los Responsables Primarios, se identificará el nivel requerido de protección. Se tomará en cuenta el caso de uso, el tipo de algoritmo de cifrado y la longitud de las claves criptográficas a utilizar.

En todos los casos se utilizarán los algoritmos enumerados en el punto 9.3.1 *Control: Política de Utilización de Controles Criptográficos.*

9.3.3 Control: Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de cualquier documento procesado electrónicamente.

La Ley Nº 25.505, de Firma Digital, el *Decreto Nº 2628/02* y un conjunto de normas complementarias, fijan competencias, establecen procedimientos y describen las condiciones bajo las cuales una firma digital es legalmente válida.

A los fines de respaldar el uso de la firma digital para su gestión interna, el MTEySS emitirá la normativa pertinente, basada en el cumplimiento de lo indicado en el párrafo anterior.

En el caso de ajenos, el MTEySS podrá intervenir, a solicitud de éstos, brindando asesoramiento y verificando el cumplimiento respecto al marco normativo aplicable.

Es importante considerar los siguientes aspectos:

- las claves criptográficas utilizadas para firma digital no deben utilizarse en procedimientos de cifrado de información,

- las claves privadas deben ser resguardarse bajo el control exclusivo de su titular. El MTEySS tomará recaudos para proteger la confidencialidad de las mismas,
- para proteger la integridad de la clave pública, el MTEySS utilizará certificados de clave pública.

9.3.4 Control: Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquel que haya originado una transacción electrónica niegue haberlo hecho.

9.3.5 Control: Protección de claves criptográficas

A los efectos de respaldar la utilización de técnicas criptográficas en el ámbito del MTEySS, se implementarán procedimientos para administrarlas.

Existen dos tipos de claves criptográficas, a saber:

- *clave secreta* (criptografía simétrica). Dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla,
- *clave pública* (criptografía asimétrica). Cada usuario tiene un par de claves: una clave pública –conocida por cualquier persona- que se utiliza para cifrar, y una clave privada –que sólo es conocida por su titular-, utilizada para descifrar.

El MTEySS deberá garantizar que todas las claves se protejan contra modificación y/o destrucción. En el caso de claves secretas y/o privadas, se implementarán protecciones contra copia y/o divulgación no autorizada.

El equipamiento utilizado para generar, almacenar y archivar claves, deberá ser clasificado como crítico o de alto riesgo.

9.3.6 Control: Protección de Claves criptográficas: Normas y procedimientos

9.3.6.1 Controles generales

Para los casos que correspondan, el MTEySS establecerá normas y procedimientos para:

- generar claves para diferentes sistemas criptográficos y aplicaciones,
- generar y obtener certificados de clave pública de manera segura,
- distribuir claves de forma segura a los usuarios que corresponda, incluyendo métodos de activación al momento de recibirlas,
- almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados,
- cambiar o actualizar claves, estableciendo reglas que indiquen el momento y el método de cambio,
- revocar claves, incluyendo cómo deben archivarse y/o desactivarse. Se considerarán contingencias tales como un compromiso de claves o cuando un usuario se desvincula del Organismo,
- recuperar claves perdidas o alteradas, como parte de los procesos de continuidad de actividades, p. ej.: para recuperar información cifrada,
- archivar claves, p. ej.: para información resguardada,
- destruir claves,
- registrar y auditar las actividades relativas a la administración de claves.

9.3.6.2 Pautas para la Administración de Claves

A fin de reducir la probabilidad de compromiso, las claves sólo podrán utilizarse dentro de un lapso establecido.

Además de la administración segura de las claves secretas y privadas, debe tenerse en cuenta la protección de las claves públicas, implementándose, a tal efecto, el empleo de certificados de clave pública.

La gestión de los certificados de clave pública debe ser absolutamente confiable. Este proceso es llevado a cabo por una tercera parte, denominada Autoridad Certificante (AC) o Certificador.

9.4 Categoría: Seguridad de los Archivos del Sistema

Objetivo

Se garantizará que las actividades de desarrollo y soporte sobre los sistemas propietarios del MTEySS se lleven a cabo de manera segura, a través del control de accesos.

Los detalles operativos de los ambientes de trabajo pueden verse en el *capítulo 7.1 Categoría: Procedimientos y Responsabilidades Operativas.*

9.4.1 Control: Software en el ambiente Operativo

9.4.1.1 Controles Generales

A fin de minimizar el riesgo de alteración de los sistemas, se definen los siguientes controles a realizar durante la implementación del software en el ambiente de producción (ver *capítulo 7.1.4 Control: Separación entre las Instalaciones de Desarrollo, Prueba, Homologación y Producción*):

- las responsabilidades inherentes a la administración del ambiente de Producción estarán a cargo del implementador, dependiente del Responsable de Informática,
- otros perfiles, tales como el Administrador de Bases de Datos, el Responsable de la Infraestructura y todo otro perfil que administre dispositivos en el ambiente operativo, serán solidariamente responsables sobre este ambiente.

9.4.1.2 Controles específicos

Deberán implementarse los siguientes controles para el ambiente de producción:

- sólo se guardarán archivos de ejecución, y los archivos de datos pertinentes,
- se definirán procedimientos para la implementación de actualizaciones, con las autorizaciones y conformidades pertinentes,
- se llevará un registro de auditoría sobre las actualizaciones realizadas,
- las versiones previas del sistema deberán retenerse, para casos de contingencia,
- ningún programador o analista de desarrollo que realice tareas de soporte de aplicaciones podrá acceder a los ambientes de producción,
- las funciones de implementación y/o administración estarán segregadas de las áreas de desarrollo y de mantenimiento de los sistemas,
- el implementador no podrá modificar los programas fuente que se hallen bajo su custodia.

9.4.2 Control: Protección de los Datos de Prueba de los Sistemas

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo, estableciéndose los siguientes procedimientos que contemplen lo siguiente (ver *capítulos 7.1.4 Control: Separación entre las Instalaciones de Desarrollo, Prueba, Homologación y Producción*):

- se efectuará una copia de la base operativa como base de prueba, mediante una autorización formal previa,
- se mantendrá un registro de auditoría de autorizaciones y accesos,

- se prohibirá el empleo de bases con datos del ambiente de producción. Sobre el ambiente de pruebas se implementará lo siguiente:
  - se mantendrá una copia actualizada de la estructura de las bases de producción,
  - se implementarán procesos de despersonalización de los datos operativos, antes de su uso,
  - se mantendrán los procedimientos de control de acceso de producción, con las autorizaciones pertinentes al ambiente de pruebas,
- una vez finalizadas las pruebas, la información utilizada en las mismas deberá eliminarse

9.4.3 Control: Cambios a Datos en el ambiente Operativo

Toda modificación, actualización o eliminación de datos operativos se efectuará a través de los sistemas que procesan dichos datos, y de acuerdo al esquema de autorizaciones y controles implementados sobre ellos (ver *Capítulo 7.1.2 Control: Cambios en las Operaciones* y *9.5.1 Control: Procedimiento de Control de Cambios*).

Se prohibirá toda modificación por fuera de los sistemas, sobre la información existente en archivos o en bases de datos. Las excepciones a la precedente política serán consideradas por el Responsable de Seguridad de la información, de acuerdo con las siguientes definiciones:

- se generará una solicitud formal para efectuar toda modificación, actualización o eliminación del dato,
- el Responsable Primario de la información afectada, junto con los Responsables de Seguridad de la Información y de Informática aprobarán la ejecución del cambio, evaluando los motivos de tal solicitud,
- se considerará la generación de cuentas de usuario de emergencia, a fin de utilizarlas exclusivamente para contingencias. Dichas cuentas estarán protegidas por contraseñas con nivel de alta criticidad, se habilitarán sólo ante un requerimiento formal y serán válidas por el lapso que dure la excepción (ver *capítulo 8.2.4 Control: Administración de Contraseñas Críticas*),
- el implementador, o quien sea designado por el Responsable de Informática, será el encargado de implementar los cambios. Se observará lo establecido en el *punto 7.1.3 Control: Separación de Funciones*),
- se registrarán todas las actividades realizadas con las cuentas de emergencia. El Responsable de Informática efectuará las revisiones de auditoría pertinentes.

9.4.4 Control: Acceso a las Bibliotecas de Programas fuentes

A fin de asegurar la integridad de los programas fuente, se aplicarán los lineamientos establecidos en el *capítulo 7.1.4 Control: Separación entre las Instalaciones de Desarrollo, Prueba, Homologación y Producción.*

Se establecerán los siguientes controles:

- el implementador administrará las bibliotecas de programa, debiendo:
  - proporcionar al personal de desarrollo los programas fuente y/o listados de rutinas ejecutables solicitados bajo procedimiento formal,
  - mantener la relación entre el programa fuente y/o rutina versos la versión ejecutable,
  - mantener un registro actualizado de todos los fuentes y rutinas ejecutables en uso, indicando nombre del programa, programador, Responsable que autorizó, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación, en producción),
  - administrar las distintas versiones de una aplicación,

- asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

- se evitará la función de administrador de programas fuente y/o rutinas de ejecutables sea ejercida por personal que pertenezca a los sectores de desarrollo y/o mantenimiento,
- se garantizará la creación automática del código ejecutable para todo programa fuente y/o rutina que pase a producción,
- se prohibirá el almacenamiento en el ambiente de producción de programas fuente y/o rutinas ejecutables que no sean los correspondientes a los programas operativos,
- estará prohibido el acceso a los operadores y/o usuarios de aplicaciones a los ambientes de desarrollo, así como a las herramientas de generación y/o manipulación de programas fuente,
- los Responsables Primarios designarán a aquellos operadores y/o usuarios de aplicaciones que accederán a los ambientes de prueba establecidos, en el marco del proceso de aceptación de un sistema (ver capítulo *7.3 Categoría: Planificación y Aprobación de Sistemas),*
- se efectuarán copias de respaldo de los programas fuente y rutinas ejecutables cumpliendo los requisitos de seguridad establecidos en el punto *7.5 Categoría: Resguardo de la información del MTEySS.*

9.5 Categoría: Seguridad de los Procesos de Desarrollo y Soporte

Objetivo

Esta Política establece las pautas de seguridad a establecer sobre los sistemas informáticos de aplicación y la información del MTEySS, verificando el control de los entornos y el soporte dado a los mismos.

9.5.1 Control: Procedimiento de Control de Cambios

A fin de mantener la integridad de los sistemas informáticos, se establecerá un estricto control de cambios, imponiendo el cumplimiento de procedimientos de seguridad y control y respetando la división de funciones (ver el *punto 7.1.2 Control: Cambios en las Operaciones,* el *punto 7.1.4 Control: Separación entre las Instalaciones de Desarrollo, Prueba, Homologación y Producción* y el *punto 9.4.1 Control: Software en el ambiente Operativo*)

Para ello, en los procesos de cambio se considerarán las siguientes pautas:

- verificar que los cambios sean propuestos por usuarios autorizados y respeten los términos y condiciones que surjan de la licencia de uso que correspondan,
- verificar que haya una autorización del Responsable Primario propietario del sistema y/o la información en cuestión,
- mantener un registro de los niveles de autorización acordados,
- todo proceso de cambio debe incluir un análisis de riesgos,
- se determinarán los aspectos de seguridad requeridos para el cambio,
- se analizará el impacto de los cambios sobre los controles de seguridad existentes,
- se verificará la aprobación del Responsable de Informática para el comienzo de las tareas vinculadas a los cambios,
- se verificará que el Responsable de Seguridad de la Información revise los cambios propuestos, a fin de garantizar el cumplimiento de los requerimientos de seguridad,
- las tareas de construcción de los cambios se efectuarán en el ambiente de desarrollo,

- aprobado el desarrollo del cambio, el testeo del mismo se efectuará en el ambiente de homologación, obteniéndose allí, de corresponder, la aprobación del usuario final y el pasaje ulterior a producción,
- actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa,
- mantener un control de versiones para todas las actualizaciones de software,
- el procedimiento de pasaje al ambiente de producción deberá tener controles que permitan minimizar la discontinuidad de las actividades y/o la alteración de los procesos involucrados,
- las áreas usuarias relacionadas deberán estar informadas antes de la implementación de un cambio que pueda afectar su operatoria.

9.5.2 Control: Revisión Técnica de los Cambios en el sistema Operativo

Todo cambio en los sistemas operativos de los servidores y puestos de trabajo del MTEySS, requerirán una revisión de los sistemas y aplicativos instalados, para evitar un impacto en el desempeño o la seguridad de la gestión operativa.

Para ello, se establecerán las siguientes pautas:

- se deberán revisar los controles de integridad y seguridad, para verificar que el cambio se genere sin compromiso sobre los datos y las aplicaciones,
- se deberá informar con la debida antelación a aquellos usuarios alcanzados por los cambios a implementar sobre los sistemas operativos,
- se deberá asegurar la actualización del Plan de Continuidad de las Actividades del Organismo, cuando corresponda.

9.5.3 Control: Restricción del Cambio de Paquetes de Software

En caso de paquetes de software suministrados por organizaciones externas y/o contratistas, se justificará la necesidad de los cambios y se emitirá una autorización previa por parte del Responsable de Informática.

Se deberá observar lo siguiente:

- analizar los términos y condiciones de la licencia, para determinar si las modificaciones se encuentran autorizadas,
- verificar obligaciones contractuales en cuanto a que la modificación sea efectuada por el MTEySS, por el organismo externo o el contratista,
- evaluar el impacto en caso que el MTEySS se haga cargo del soporte,
- verificar la existencia de procesos de retención del software original. Los cambios se efectuarán sobre una copia perfectamente identificada, y contando con documentación exhaustiva, por si fuera necesario aplicarlos a nuevas versiones.

9.5.4 Control: Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información del MTEySS, utilizando medios no autorizados, indirectos y desconocidos. El código malicioso, por otra parte, está diseñado para afectar a un sistema en forma no requerida por el usuario.

En este sentido, se establecerán las siguientes pautas:

- como parte del proceso de pruebas y antes de la aprobación para la instalación en producción, deben examinarse los códigos fuente, siempre que sea posible,
- deberá examinarse la existencia de controles de seguridad en el código, en forma previa a la puesta en producción.

- se deberán implementar procedimientos periódicos de evaluación de seguridad en el código instalado,
- se deberán utilizar herramientas para la protección contra la infección del software con código malicioso,
- se deberán controlar los accesos y las modificaciones a todo código instalado,
- se deberán adquirir paquetes de software a proveedores acreditados, y los productos deben presentar evaluaciones previas.

9.5.5 Control: Desarrollo Externo de Software

Para los casos en que se recurra a organizaciones externas y/o contratistas para el desarrollo de software, se establecerán procedimientos que contemplen las siguientes pautas:

- implementación de acuerdos de licencia, estableciendo la propiedad del código y los derechos que se confieren (Ver *capítulo 12.1.2 Derechos de Propiedad Intelectual*).
- definición de requerimientos contractuales respecto de aspectos de calidad y seguridad del código, y la presencia de garantías,
- definición de procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, incluyendo:
  - auditorías y revisión de código para detectar código malicioso,
  - verificación del cumplimiento de los requerimientos de seguridad del software.
- implementación de acuerdos para la custodia de los archivos fuente, y toda la documentación pertinente, en caso de quiebra del proveedor.

9.6 Categoría: Gestión de vulnerabilidades técnicas

Objetivo

Se deberá mantener un control sobre las vulnerabilidades técnicas de los sistemas operativos y las aplicaciones informáticas.

Se dispondrá de un proceso de gestión sistemático y repetible, con métricas que permitan confirmar su efectividad (ver *capítulo 4. Evaluación y tratamiento de riesgos*).

9.6.1 Control: Vulnerabilidades técnicas

Se deberá disponer de información actualizada acerca de las vulnerabilidades técnicas de los sistemas informáticos instalados, así como la exposición del MTEySS y los riesgos emergentes. Se evaluarán e implementarán las medidas de tratamiento adecuadas.

Se deberá disponer de un inventario de software donde se detalle toda la información pertinente, p. ej.: versiones instaladas, Responsables Primarios, proveedor –en caso de paquetes de software-, y responsables de desarrollo.

El proceso de gestión de las vulnerabilidades técnicas debe incluir lo siguiente:

- definición, por parte del Responsable de Seguridad de la Información, de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas,
- procedimientos de identificación y evaluación de vulnerabilidades técnicas potenciales, considerando los riesgos asociados y las acciones factibles de llevar a cabo,
- definición de un procedimiento de tratamiento de vulnerabilidades técnicas potencialmente relevantes, estableciendo:
  - notificaciones,
  - tiempos de respuesta,
  - métodos de tratamiento.

- definición de prioridades para la atención de las actualizaciones de seguridad,
- identificación de los riesgos asociados a la instalación de parches,
- procedimientos de evaluación y aprobación de los parches, antes de su instalación,
- definición de controles compensatorios en caso de inexistencia de parches,
- implementación de procedimientos de auditoría, seguimiento y evaluación regular.

10. Cláusula: Gestión de Incidentes de Seguridad

Generalidades

El MTEySS cuenta con activos de información que se hallan expuestos a sufrir un compromiso a su seguridad.

Se debe contar, por ende, con una capacidad de gestión tal que, empezando por la detección, se lleve a cabo un tratamiento y una prevención futura de amenazas que, al materializarse, provoquen incidentes que afecten la seguridad de la información.

Objetivo

Se debe garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas se detecten y comuniquen de tal forma que se apliquen las acciones correctivas en el momento oportuno.

Alcance

La política definida en esta cláusula alcanza a todos los activos de información del MTEySS, incluyendo a todos sus usuarios.

Responsabilidad

El Comité de Seguridad de la Información definirá y recomendará la implementación de medios y canales necesarios para que los Responsables de Seguridad de la Información y de Informática, donde corresponda, gestionen los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité tomará conocimiento de los incidentes relativos a la seguridad, impulsando las acciones tendientes a su resolución.

Los Responsables de Seguridad de la Información y de Informática, donde corresponda, tienen a cargo el seguimiento, la documentación y el análisis de los incidentes de seguridad reportados, así como la investigación de amenazas que puedan impactar sobre la seguridad de los datos del MTEySS. Asimismo, debe efectuar informar y efectuar recomendaciones para tomar acciones de resolución, tanto a los responsables Primarios y como al Comité de Seguridad de la Información.

El Responsable de Recursos Humanos colaborará con el Responsable de Seguridad de la Información en la comunicación fehaciente al personal, organizaciones externas y/o contratistas, cuando corresponda, sobre los procedimientos de gestión de incidentes de seguridad.

El Responsable del Área Legal participará en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo aquel que utilice activos de información del MTEySS colaborará en la tarea de reportar debilidades e incidentes de seguridad que oportunamente se detecten.

Política

10.1 Categoría: Informe de los eventos y debilidades de la seguridad de la información

Objetivo

Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información se comuniquen de tal forma de llegar a implementar acciones correctivas en el momento adecuado.

10.1.1 Control: Reporte de los eventos de la seguridad de información

Todo incidente relativo a la seguridad será comunicado a través de las autoridades o los canales que éstas designen, tan pronto como sea posible, mediante un procedimiento formal. Se indicará la acción que ha de emprenderse al recibir un informe sobre incidentes.

Todo aquel que haga uso de los recursos de información del MTEySS tomará conocimiento del procedimiento de comunicación de incidentes de seguridad.

Al respecto, se buscará la colaboración del Programa Nacional de Infraestructuras Críticas de Información a los fines de obtener respuestas ante incidentes de seguridad que afecten a los recursos informáticos del Organismo.

Ante la detección de un posible incidente o violación de seguridad, los usuarios informarán formalmente a los Responsables de Seguridad de la Información y el Responsable de Informática, donde corresponda, quienes deberán contemplar lo siguiente:

- definir los recursos necesarios para la investigación y resolución del incidente,
- recomendar las acciones a implementar, y efectuar monitoreo sobre las mismas,
- informar a los Responsables Primarios y al Comité de Seguridad de la Información sobre las gestiones y los resultados obtenidos.

10.1.2 Control: Reporte de las debilidades de la seguridad

Los usuarios de los recursos de información del MTEySS deben comunicar, rápidamente y de manera formal, sobre las fallas de seguridad que hayan detectado.

Sin perjuicio de lo anterior, los usuarios tienen prohibido:

- la realización de pruebas para detectar y/o aprovechar una supuesta debilidad o falla de seguridad,
- toda operación sobre los datos y/o el software afectados, hasta tanto no se haya resuelto el incidente.

10.1.3 Control: Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los que deben contemplar:

- la registración de síntomas del problema y mensajes que aparecen en pantalla,
- la definición de medidas de aplicación inmediata ante la presencia de una anomalía,
- el alerta inmediato y formal a los Responsables de Seguridad de la Información y de Informática, donde corresponda, y al Responsable Primario pertinente.

10.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información

Objetivo

Se debe asegurar que los incidentes en la seguridad de la información sean manejados de manera efectiva y eficiente, desde el momento de la detección de eventos, pasando por la comunicación a las partes involucradas y finalizando el tratamiento para lograr su resolución.

Se deben establecer las responsabilidades y los procedimientos para la gestión de incidentes de seguridad, aplicando conceptos de mejora continua para la detección, la evaluación, la respuesta y el monitoreo.

10.2.1 Control: Responsabilidades y procedimientos

Los Responsables de Seguridad de la Información y de Informática, cuando corresponda, establecerá funciones y procedimientos de tratamiento, de forma de garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad En los casos que corresponda, se solicitará la participación del Responsable del Área Legal.

Se deben considerar los siguientes ítems:

- determinar, investigar y verificar las amenazas probables de crear incidentes de seguridad en el MTEySS, incluyendo, entre otros, los siguientes tipos:
  - fallas operativas,

- código malicioso,
- intrusiones,
- fraude informático,
- error humano,
- catástrofes naturales.

- establecer procedimientos de comunicación formal y oportuna, a los Responsables Primarios, al Responsable de Informática, a las Autoridades y usuarios en general, donde corresponda, utilizando los canales apropiados,
- definir planes de contingencia, donde se contemplarán siguientes puntos:
  - análisis e identificación de la causa del incidente,
  - definición de las primeras medidas a implementar,
  - planificación e implementación de soluciones,
  - comunicación formal con las personas afectadas,
  - convocar a las personas afectadas a las tareas de recuperación, conde corresponda,
- implementar controles acerca de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
  - otorgar acceso a los sistemas y datos afectados sólo al personal taxativamente autorizado por los Responsables de Seguridad de la Información y de Informática, donde corresponda, con el acuerdo del Responsable Primario,
  - documentar en forma detallada todas las acciones de emergencia emprendidas,
  - comunicar las acciones de emergencia al Responsable Primario de la información afectada,
  - efectuar una revisión de cumplimiento de las acciones implementadas,
  - verificar la integridad de los sistemas, datos y controles restablecidos, en un plazo mínimo.
- establecer procedimientos de registro de pistas de auditoría y/o evidencia similar para:
  - disponer de información histórica que permita evitar la repetición del mismo incidente,
  - efectuar análisis de problemas internos,
  - disponer el estudio de factibilidad de mejora o incorporación de nuevos controles,
  - disponer de evidencia en relación con una posible violación contractual, infracción normativa, o en el marco de un proceso judicial (Ver *capítulo 12.1. Categoría: Cumplimiento de Requisitos Legales*).

10.2.2 Control: Aprendiendo a partir de los incidentes de seguridad de la información

Los Responsables de Seguridad de la Información y de Informática establecerán un proceso que permita monitorear, documentar y cuantificar los tipos eventos y anomalías, de manera de identificar los incidentes recurrentes o aquellos que tengan alto impacto.

Con la información obtenida se efectuarán evaluaciones que determinarán la necesidad de mejorar o agregar controles, a fines de limitar la frecuencia, el daño posible y los costos de resolución de casos futuros.

10.2.3 Control: Procesos Disciplinarios

Para el caso de personal del MTEySS que viole las políticas, normas, procesos y procedimientos de seguridad de la información, se seguirán los procedimientos disciplinarios formales que

correspondan, según la normativa vigente para las personas afectadas a la Administración Pública Nacional.

11. Cláusula: Gestión de la Continuidad

Generalidades

La administración de la continuidad de las actividades es un proceso crítico, y debe involucrar a todos los niveles de autoridad y operaciones del MTEySS.

La implementación de planes de contingencia y continuidad garantizará que las actividades del MTEySS se restablezcan en un plazo aceptable para mantener la gestión y las operaciones que le competen a esta cartera de Estado.

Los planes deben desarrollarse, ensayarse y actualizarse en un contexto de integración con el resto de los procesos de administración y gestión.

La gestión de la continuidad debe incluir controles destinados a:

- identificar y mitigar riesgos,
- atenuar las consecuencias de eventuales interrupciones de las actividades del MTEySS,
- asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

Los objetivos de esta cláusula son:

- minimizar los riesgos y el impacto de las posibles interrupciones en las actividades normales del MTEySS,
- proteger los procesos críticos mediante una combinación de controles preventivos y correctivos,
- analizar las consecuencias de la interrupción del servicio, corregir las fallas y tomar las medidas correspondientes para la prevención de hechos futuros del mismo tenor,
- maximizar la efectividad de la ejecución de los planes de contingencia del MTEySS, los cuales deben incluir, como mínimo, las siguientes etapas:
    - notificación/activación. Consistente en la detección del daño y su impacto, así como la puesta en marcha de las actividades de contingencia planificadas,
    - reanudación. Consistente en la ejecución de procedimientos de emergencia que permitan que el sistema dañado pueda recuperarse del daño producido y se reestablezcan las operaciones del MTEySS,
    - recuperación. Consistente en la restauración de la capacidad de procesamiento del sistema dañado a las condiciones de operación normales,
    - asegurar la coordinación del personal del MTEySS con los contactos externos que participarán en las estrategias de planificación de contingencias, cuando corresponda. Se deberá asignar funciones para cada actividad definida.

Alcance

Esta Política se aplica a todos los procesos y datos del MTEySS clasificados como críticos (ver *capítulo 4.2 Categoría: Clasificación de la información*).

Responsabilidad

Los Responsables de Informática, y de Seguridad de la Información, participarán activamente en la definición, documentación, prueba y actualización de los planes de contingencia y continuidad.

El Comité de Seguridad de la Información verificará y aprobará la gestión de continuidad de las operaciones del MTEySS frente a interrupciones imprevistas.

Los Responsables Primarios revisarán periódicamente los planes bajo su incumbencia, como así también identificarán cambios en las disposiciones relativas a las actividades del MTEySS aún no

reflejadas en los planes de continuidad. Asimismo, deberán verificar el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan.

Los Responsables Primarios, junto con el Responsable de Seguridad de la Información, cumplirán las siguientes funciones:

- identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del MTEySS,
- evaluar los riesgos, a fin de conocer el impacto de las interrupciones,
- identificar los controles preventivos existentes,
- elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del MTEySS,
- considerar el enfoque global con el que se abordará la continuidad de las actividades del MTEySS, de forma de integrar los distintos planes.

Política

11.1 Categoría: Gestión de continuidad del Organismo

Objetivo

Se implementarán acciones que permitan mitigar los efectos de fallas o desastres sobre los activos de información, asegurando la reanudación de las actividades críticas del MTEySS.

11.1.1 Control: Proceso de Administración de la continuidad del Organismo

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del MTEySS.

Los Responsables de Informática y de Seguridad de la Información informarán al Comité de Seguridad sobre la gestión de las operaciones de continuidad y/o contingencia frente a interrupciones imprevistas.

La gestión de continuidad deberá incluir lo siguiente:

- identificación de los procesos y activos de información del MTEySS clasificados como críticos,
- elaboración de planes de continuidad y contingencia sobre la gestión del MTEySS, junto con los Responsables Primarios pertinentes, incluyendo actividades de concientización a los usuarios,
- integración de los distintos planes de contingencia y continuidad existentes en el MTEySS en función de una estrategia común,
- elaboración de un cronograma de pruebas periódicas de cada uno de los planes de contingencia y continuidad, proponiendo una asignación de funciones para su cumplimiento,
- implementación de actualizaciones periódicas de los planes y procesos implementados,
- empleo de servicios de organizaciones externas o contratistas, como los seguros o la guarda externa de medios de resguardo, a los fines de la integración con los procedimientos de continuidad y contingencia.

11.1.2 Control: Continuidad de las Actividades y Análisis de los impactos

La planificación de la continuidad de las actividades, así como el análisis del impacto por interrupciones a los servicios del MTEySS, serán llevados a cabo por los Responsables de Seguridad de la Información y de Informática, cuando corresponda, con la activa participación de los Responsables Primarios, los Responsables de Seguridad Física y del área Administrativa, según corresponda.

Tomando como base lo establecido en el *capítulo 3. Evaluación y tratamiento de riesgos*, en la elaboración de los planes de gestión de continuidad y contingencia se deben contemplar los siguientes puntos:

- identificación de eventos y/o amenazas que puedan ocasionar interrupciones en los procesos, p. ej.: fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación y/o incendio, desastres naturales, destrucción edilicia y terrorismo, entre otros,
- evaluación de riesgos, a fin de determinar el impacto de los cortes, tanto en términos de magnitud de daño como de tiempos requeridos para la recuperación. Dicha evaluación identificará los recursos críticos, el impacto producido por una interrupción, los tiempos de interrupción aceptables o permitidos, y las prioridades de recuperación,
- identificar controles preventivos, tales como: sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de resguardo, registros de auditoría, controles de acceso, entre otros.

11.1.3 Control: Elaboración e implementación de los planes de continuidad de las Actividades del Organismo

El Responsable de Seguridad de la Información, el Responsable de Seguridad Física, el Responsable de Recursos Humanos, y los Responsables Primarios, donde corresponda, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del MTEySS. Los planes serán revisados y coordinados por el Comité de Seguridad de la Información.

La gestión de continuidad y resolución de contingencias considerará los siguientes puntos:

- identificar y acordar respecto a todas las funciones y procedimientos de emergencia requeridos,
- analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso, considerando:
  - servicios y recursos disponibles para la reanudación de las actividades,
  - determinación de plazos de reanudación adecuados a los objetivos de gestión esperados,
  - formación de los equipos técnicos asignados a las tareas de reanudación y/o recuperación,
  - acuerdos para reanudación de emergencia en sitios de procesamiento alternativos.
- implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe considerar muy especialmente la dependencia entre servicios, para determinar las prioridades y el orden adecuado de restablecimiento de los servicios,
- se debe dedicar especial atención a la relación entre actividades externas e internas del MTEySS, así como los contratos y/o acuerdos vigentes,
- documentar los procedimientos y procesos acordados,
- capacitar adecuadamente al personal, en materia de manejo de emergencias y crisis, así como en la reanudación y la recuperación de los sistemas afectados, considerando:
  - objetivo del plan de contingencias y continuidad,
  - mecanismos de coordinación y comunicación entre las áreas involucradas,
  - procesos específicos para el personal involucrado,
  - procedimientos de divulgación al personal y usuarios del MTEySS,
  - responsabilidades individuales,

- requisitos de seguridad física, de los recursos humanos y del equipamiento informático.

- ensayar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

11.1.4 Control: Marco para la Planificación de la continuidad de las Actividades del Organismo

Si bien podrán definirse varios planes de continuidad, se mantendrá un único marco de referencia, de manera que, ante un evento, haya una adecuada coordinación entre áreas del MTEySS y se permita una correcta identificación de prioridades y líneas de acción.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos establecidos, p. ej.: los planes de evacuación o los recursos de emergencia existentes.

El Responsable de Seguridad de la Información, junto con el Comité de Seguridad, analizará la formulación de cada plan, verificando que haya una correlación común entre todos. A su vez, cada Responsable Primario designará a un administrador para el plan de continuidad a su cargo, siendo éste el encargado de coordinar las tareas definidas en el mismo.

El marco para la planificación de la continuidad de las actividades del Organismo, deberá considerar los siguientes puntos:

- prever los requisitos que permitan describir el proceso a seguir, antes de poner en marcha el plan, p. ej. :
  - cómo evaluar la situación,
  - qué personas estarán involucradas,
  - con qué recursos se cuenta.
- definir los procedimientos para implementar las acciones de emergencia a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del MTEySS y/o la vida humana. Se deben considerar aspectos como: la gestión de las relaciones públicas y los vínculos con organismos tales como, p,. ej.: policía, bomberos y/o autoridades locales, según corresponda,
- documentar los procedimientos que describan:
  - las acciones de emergencia a emprender en caso de traslado de actividades y servicios críticos a ubicaciones transitorias alternativas,
  - los plazos requeridos para el adecuado restablecimiento de los procesos de gestión del MTEySS.
- documentar los procedimientos que describan las acciones de recuperación a emprender en los sitios de procesamiento del MTEySS,
- establecer un cronograma que especifique cómo y cuándo será probado el plan,
- establecer un procedimiento de mantenimiento y mejora del plan,
- documentar las responsabilidades y funciones de las personas involucradas en el plan. Se indicará lo siguiente:
  - definir los diferentes planes de contingencia, y registrar a los respectivos administradores,
  - describir a los responsables de la ejecución de cada uno de los componentes del plan,
  - establecer vías y prioridades para establecer contacto con los involucrados,
  - designar al responsable de declarar el estado de contingencia, dando así inicio al plan que corresponda.

- efectuar actividades de capacitación al personal involucrado, de forma de propiciar la comprensión de los procesos de continuidad y garantizar su eficacia.

11.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del MTEySS

Los planes de continuidad de las actividades del MTEySS deben ser revisados y actualizados periódicamente, para garantizar su eficacia permanente.

En tal sentido, es necesario efectuar pruebas y revisiones de funcionamiento de los planes de continuidad (ver *capítulo 10.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información*), a fin de prever fallas o errores que, en la ejecución de dichos planes, produzcan un impacto sobre la protección de los datos del MTEySS.

11.1.5.1 Responsabilidades

Se establecerán las siguientes responsabilidades:

- los administradores de los planes de continuidad y contingencia, junto con el Responsable de Seguridad de la Información, tendrán a su cargo las revisiones periódicas de cada uno de los planes de su incumbencia,
- los administradores de los planes de continuidad y contingencia deberán identificar los aquellos cambios en las actividades del MTEySS que deban reflejarse en cada uno de los planes de su incumbencia, ,
- el Responsable de Seguridad de la información, junto con los administradores, presentará al Comité de Seguridad de la Información un cronograma de pruebas periódicas para cada uno de los planes de contingencia y continuidad,
- los administradores gestionarán la realización de las pruebas, indicando quiénes son los responsables de llevarlas a cabo y presentando los resultados obtenidos al Responsable Primario competente, al Responsable de Seguridad de la Información y al Comité de Seguridad.

11.1.5.2 Verificación del funcionamiento de los planes de continuidad

Debe garantizarse que los planes de contingencia funcionen ante un hecho real, para lo cual deben establecerse ensayos y verificaciones periódicas.

Los procedimientos de verificación deben contemplar la documentación de las pruebas, así como el resguardo de la evidencia formal de la ejecución y de los resultados obtenidos.

Se deben considerar, como mínimo, las siguientes técnicas:

- *pruebas de discusión*: proponiendo distintos escenarios de contingencia, se discutirán y evaluarán, en forma teórica, las medidas de recuperación y pruebas a efectuar ante posibles ejemplos de interrupciones,
- *simulaciones*: el personal involucrado analizará rutinas y roles en la gestión de recuperación, en sesiones de práctica, a fines de evaluar el grado de preparación del personal para enfrentar un incidente o un desastre simulado.
- *pruebas de recuperación técnica*: las mismas permitirán medir el grado de eficacia en las acciones de restablecimiento de un sistema,
- *ensayo completo:* planteando una supuesta situación de crisis, todo el personal involucrado ejecutará el plan de contingencias, ejerciendo el rol que ocupará en una emergencia. Este ensayo puede incluir una interrupción parcial o total de los servicios.

Para las operaciones críticas del Organismo se tomarán en cuenta, además, los siguientes mecanismos:

- pruebas de recuperación en paralelo. Se ejecutan las pruebas del plan en paralelo a las actividades, través de ensayos de recuperación en un sitio alternativo, de ser posible,

- pruebas de servicios de proveedores. Se ejecutan los planes sobre los productos y servicios prestados por los proveedores externos, para medir el grado de cumplimiento de los compromisos contraídos.

11.1.5.3 Actualizaciones a los planes de continuidad

Los procedimientos de gestión de cambios deben garantizar que se aborde adecuadamente lo atinente a la continuidad de actividades en el MTEySS.

Las modificaciones a los planes serán evaluadas por los administradores, junto con el Responsable de Seguridad de la Información. A posteriori, la propuesta se elevará al Comité de Seguridad de la Información para su aprobación por parte de las Autoridades.

Por otra parte, los procedimientos asegurarán la adecuada comunicación de los cambios a todo el personal involucrado.

Debe prestarse atención, especialmente, a los cambios de: personal, estrategias del MTEySS, ubicación física de instalaciones y recursos, direcciones y números telefónicos, normativa y legislación, proveedores y contratistas, procesos nuevos o eliminados, tecnologías, requisitos operacionales, requisitos de seguridad, registros y datos críticos.

12. Cláusula: Cumplimiento

Generalidades

El MTEySS debe garantizar el cumplimiento de las disposiciones normativas y legales que regulan el acceso a la información almacenada y procesada en su ámbito.

Objetivos

Los objetivos de esta cláusula son:

- establecer la obligatoriedad en el cumplimiento de las disposiciones normativas y legales que se corresponden con los objetivos organizacionales del MTEySS,
- tomar conocimiento de las sanciones administrativas, así como de las responsabilidades civiles y/o penales pasibles de ser aplicadas en caso de incumplimiento,
- garantizar que los sistemas de información y las plataformas tecnológicas cumplan efectivamente con las políticas, normas y procedimientos de seguridad del MTEySS,
- revisar periódicamente las políticas de seguridad de la información, de manera que el MTEySS esté actualizado en lo referido a la adecuada protección de sus datos y recursos,
- verificar la eficacia del proceso de auditoría de sistemas, de tal forma de minimizar los riesgos y los obstáculos que pudieran afectarlo,
- garantizar la existencia de controles que protejan los datos en el transcurso de las auditorías de sistemas,
- determinar los plazos para la guarda de información y la recolección de evidencia.

Alcance

Esta Política se aplica a:

- todo el personal del MTEySS, cualquiera sea su situación de revista,
- quienes accedan a datos o utilicen recursos de información de esta cartera de Estado,
- los sistemas de información y sus plataformas tecnológicas,
- las normas, los procedimientos, los datos, la documentación generada y las auditorías efectuadas sobre los sistemas.

Responsabilidad

El Área Legal establecerá los aspectos jurídicos y legales relacionados con la seguridad de la información, así como sobre las responsabilidades individuales emanadas del cumplimiento de dichos aspectos.

El Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- definir normas y procedimientos que garanticen el cumplimiento de las restricciones legales respecto del uso de la información del MTEySS,
- realizar revisiones periódicas sobre las áreas del MTEySS a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad de la información. Esta tarea se efectuará con la colaboración de los Responsables Primarios, el Responsable de Informática, los Responsables de Recursos Humanos y de Seguridad Física, cuando corresponda,
- verificar periódicamente que los sistemas de información cumplan con las políticas, las normas y los procedimientos de seguridad establecidos,
- garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable del Área Legal, con la asistencia del Responsable de Seguridad de la Información, cumplirá las siguientes funciones:

- definir y documentar los requisitos normativos y contractuales pertinentes para cada sistema de información,
- establecer los Compromisos de Confidencialidad a ser firmados por todo el personal, organizaciones externas y/o contratistas que accedan a la información del MTEySS.

Los Responsables Primarios velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

Todo el personal, sin importar su nivel jerárquico, así como las terceras partes o ajenos que accedan a información del MTEySS, deberán conocer, divulgar, cumplir y hacer cumplir las presentes políticas y la normativa competente.

Política

12.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo

Asegurar la observancia de las leyes, normas y todo requerimiento relacionado con la seguridad, y con el uso y la gestión de los recursos y sistemas de información del MTEySS.

12.1.1 Control: Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

12.1.2 Control: Derechos de Propiedad Intelectual

Se deberá garantizar el cumplimiento de los aspectos legales relacionados con la propiedad intelectual de datos y/o sistemas empleado en el MTEySS.

El MTEySS sólo podrá autorizar a que los usuarios usen material, sea desarrollado internamente, sea cedido por un organismo externo o adquirido a un contratista, conforme los términos y condiciones acordadas y según lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deben tener presentes las siguientes normas: Ley de Propiedad Intelectual Nº 11.723, Ley de Marcas Nº 22.362, Ley de Patentes de Invención y Modelos de Utilidad Nº 24.481,

12.1.2.1 Derecho de Propiedad Intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la *Ley 11.723 de Propiedad Intelectual.* Dentro del software se incluyen: listados de programas fuente y compilables, listados de rutinas ejecutables, así como los contratos de licencia para su uso, reproducción y/o copia.

El Responsable de Seguridad de la Información, con la asistencia del Responsable de Informática y del Área Legal, analizará los términos y condiciones de licencia, a fines de implementar lo siguiente:

- normas y procedimientos para el cumplimiento del derecho, a los fines del uso legal de productos de información y de software, a saber:
  - establecer los términos y condiciones para ceder derechos de uso del software propietario, desarrollado en el MTEySS, a organizaciones externas y contratistas, donde corresponda,

- divulgar los términos y condiciones establecidos para los contratos de adquisición de software y distribución de licencias, en función de la Ley de Propiedad Intelectual, donde corresponda,
- establecer y notificar las acciones disciplinarias, administrativas y/o penales que correspondan ser aplicadas contra quien las infrinja.

- registro de activos y evidencias de propiedad de licencias,
- mecanismos de guarda en condiciones seguras de licencias, discos maestros, manuales y documentación pertinente,
- límites establecidos para el número máximo permitido de usuarios,
- controles para habilitar la instalación de productos con licencia y software autorizado, únicamente,
- procedimientos que establezcan la transferencia de software propietario a organizaciones externas y/o contratistas, donde corresponda,
- establecer términos y condiciones establecidos para obtener software e información en redes públicas,
- establecer herramientas de auditoría adecuadas.

12.1.3 Control: Protección de los Registros del Organismo

Los registros críticos del MTEySS deben protegerse contra pérdida, destrucción y falsificación. Asimismo, deben establecerse procedimientos de retención segura, a los fines de cumplir requisitos legales y/o normativos, y respaldar las actividades esenciales del Organismo.

Los registros deberán tener asignado un período de guarda y retención, debiendo conocerse, asimismo el tipo de medio en que se almacena, a saber: papel, microfichas, medios magnéticos u ópticos.

Los registros se clasificarán en los siguientes tipos: registros contables, registros de base de datos, claves criptográficas registros de auditoría y procedimientos operativos, entre otros.

Los Responsables Primarios, donde corresponda, deberán designar un encargado de gestión de los registros.

12.1.3.1 Preservación de registros

El Responsable de Seguridad de la Información establecerá procedimientos que garanticen una adecuada preservación de los registros.

En base a lo indicado en el *Capítulo 7.7 Categoría: Administración y Seguridad de los medios de almacenamiento*, se deberán adoptar las siguientes medidas:

- elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información,
- establecer un cronograma de retención que tenga en cuenta los tipos de registro y el período durante el cual deben ser retenidos,
- establecer controles que permitan que los registros estén protegidos contra pérdida, destrucción y/o falsificación.

12.1.3.2 Normativa Relacionada

En particular, se deben tener presente las siguientes normas:

- *Ética en el Ejercicio de la Función Pública. Ley 25.188*, a fin de proteger y conservar la propiedad del Estado, y el uso de los bienes con fines autorizados,
- *Código de Ética de la Función Pública*, a fin de disponer la obligación de los funcionarios en cuanto a la protección y el uso adecuado de los bienes del Estado,

- *Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164*: Establece el deber de los funcionarios públicos de observar fidelidad y mantener reserva respecto de sus tareas y de la información a la que acceden,
- *Código Penal Art. 255*, a fin de establecer sanciones para quien sustraiga, oculte o destruya evidencia,
- *Ley Nº 24.624. Artículo 30*, a fin de definir la utilización del soporte electrónico que garantice estabilidad, perdurabilidad, inmutabilidad e inalterabilidad,
- *Decisión Administrativa 43/96*, reglamentando el Art. 30 de la Ley 24.624, a fin de determinar un ámbito de aplicación, conceptos y requisitos relacionados con la elaboración de documentos y su soporte,
- *Ley Nº 25.506*, a fin de establecer el uso de firma digital en la documentación,
- *Código Penal Art 183*, a fin de establecer sanciones para quien altere, destruya o inutilice datos, documentos, programas o sistemas de información,
- *Decreto 1172/2003*, a fin de establecer las pautas de acceso a la información de carácter público.

12.1.4 Control: Protección de Datos y Privacidad de la Información Personal

Se deben establecer controles para que la información del MTEySS sea utilizada por el personal -sin importar su nivel jerárquico-, y los ajenos que lo requieran, para fines específicos previamente definidos.

Sólo se divulgará, procesará y/o comunicará aquella información del MTEySS que esté autorizada previamente por el Responsable Primario a cargo.

Por otra parte, y según lo establecido en el *punto 6.1.4 Control: Compromisos de confidencialidad*, el MTEySS se reserva el derecho de efectuar control y monitoreo sobre las actividades ejercidas en su ámbito, preservando el derecho a la privacidad del empleado, según corresponda.

En particular, se deben tener presentes las siguientes normas:

- *Protección de Datos Personales. Ley 25.326*, establece responsabilidades y criterios para procesar, divulgar y/o ceder datos personales,
- *Confidencialidad Ley Nº 24.766*, impide la divulgación a terceros, o su utilización sin previo consentimiento, de información secreta,
- *Delitos Informáticos Ley N° 26.388*, modifica el Código Penal, de forma de incorporar al mismo diversos delitos informáticos, tales como violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático, interrupción de comunicaciones además de distribución de virus y pornografía infantil,

12.1.5 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del MTEySS se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

El alcance preciso del uso adecuado se definirá según lo indicado en el *capítulo 5.2.4 Control: Compromiso de Confidencialidad y Uso Adecuado de los recursos de información.*

12.1.6 Control: Regulación de Controles para el Uso de Criptografía

En la utilización de firmas digitales o electrónicas, el MTEySS deberá observar lo dispuesto por la *Ley 25.506, su decreto reglamentario Decreto 2628/02*, y la normativa interna emitida a tal fin, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

12.1.7 Control: Recolección de Evidencia

Se establecerán procedimientos para la preservación de los datos y registros del MTEySS, de forma que su recuperación produzca evidencia válida ante un tribunal de justicia.

Para lograr la validez de la evidencia, el MTEySS deberá observar lo indicado en los capítulos *4.3 Categoría: Etiquetado y Manipulación de la información, 7.5 Categoría: Resguardo de la información del MTEySS, 7.7 Categoría: Administración y Seguridad de los medios de almacenamiento* y *7.10.2 Control: Protección de los registros.*

12.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica

Objetivo

Se debe asegurar que los sistemas de información del MTEySS cumplan con la normativa de protección de sus datos. Para ello, el MTEySS establecerá un proceso de revisión periódica de las políticas de seguridad de la información.

Esta revisión debe surgir como resultado de la actualización de la normativa nacional e internacional que entiende en el tema, así como del avance de nuevas técnicas para la protección de la información y la implementación de nuevos sistemas en el ámbito del MTEySS.

12.2.1 Control: Cumplimiento de la Política de Seguridad

El Responsable de Seguridad de la Información, con la colaboración de los Responsables Primarios, de Informática y de Seguridad Física, efectuará un monitoreo sobre los controles del MTEySS que permitan verificar el cumplimiento de la política, las normas y los procedimientos de seguridad.

Se verificarán los sistemas de información, los accesos de los usuarios, el cumplimiento de los compromisos de confidencialidad y el funcionamiento de los perímetros de seguridad del MTEySS, entre otros.

12.2.2 Control: Verificación de la Compatibilidad Técnica

El Responsable de Seguridad de la Información efectuará una revisión periódica de los sistemas en producción, a fin de garantizar que los controles de seguridad hayan sido correctamente implementados. De ser necesario, se podrá recurrir a un servicio externo de asistencia técnica especializada.

La verificación del cumplimiento comprenderá ensayos –conocidos como pruebas de penetración- cuyos objetivos serán la detección de vulnerabilidades y la verificación de la eficacia de los controles de seguridad en los sistemas del MTEySS. Se establecerán procedimientos formales que garanticen la planificación, la ejecución ordenada y la debida divulgación de informes a las partes interesadas

12.3 Categoría: Consideraciones de Auditorías de Sistemas

Objetivo

Se buscará maximizar la efectividad de los procesos de auditoría, a la par de minimizar el impacto que el proceso de auditoría tenga sobre el sistema de información auditado. Para ello, deberán implementarse controles a los fines de salvaguardar los sistemas y herramientas de auditoría.

Para la implementación de las actividades de auditoría, se aplicarán las Normas de Control Interno para Tecnologías de Información, aprobadas por la *resolución SIGEN Nº 48/05.*

12.3.1 Control: Controles de Auditoría de Sistemas

Toda actividad de auditoría sobre sistemas en producción, deberá ser planificada y coordinada adecuadamente con los Responsables Primarios pertinentes. Con ello se buscará minimizar riesgos por interrupción en las operaciones del MTEySS.

Se contemplarán los siguientes puntos:

- los requerimientos de auditoría se acordarán con los Responsables Primarios, el Responsable de Seguridad de la Información y el Responsable de Informática, donde sea pertinente,
- la Unidad de Auditoría Interna, o quien sea propuesto por el Comité de Seguridad de la Información, será quien deba controlar el alcance de las verificaciones,
- las verificaciones a efectuar sobre software y datos de producción deberán estar limitadas a un acceso de sólo lectura,
- en casos que el proceso de auditoría requiera efectuar modificaciones de datos y/o software en producción, se deberán tomar los siguientes recaudos, una vez finalizada la auditoría:
  - eliminar archivos transitorios,
  - eliminar entidades ficticias y datos incorporados en archivos y bases maestras,
  - revertir transacciones,
  - revocar privilegios otorgados.
- la Unidad de Auditoría o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, indicará cuáles son los recursos tecnológicos necesarios para efectuar las verificaciones de auditoría, los que serán provistos por el Responsable de Informática,
- las actividades de auditoría deben estar monitoreadas, debiendo registrarse, como mínimo, la siguiente información:
  - fecha y hora,
  - puesto de trabajo,
  - usuario,
  - tipo de acceso,
  - identificación de los datos accedidos,
  - estado previo y posterior,
  - programa y/o función utilizada.
- documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

12.3.2 Control: Protección de los Elementos Utilizados por la Auditoría de Sistemas

Los archivos de datos y software utilizados en las actividades de auditoría deben protegerse, a fin de evitar un mal uso o compromiso sobre los mismos.

Las herramientas e auditoría deben separarse de los sistemas en producción y/o desarrollo. A tal efecto, se tomarán los recaudos necesarios a efectos de cumplir con las normas dispuestas por la Sindicatura General de la Nación.

12.3.3 Control: Sanciones Previstas por Incumplimiento

Todo aquel que viole lo dispuesto en la presente Política de Seguridad se encontrará sujeto a sanciones conforme a lo dispuesto por la legislación y las normas y convencionales que rigen tanto al personal de la Administración Pública Nacional como a aquellas organizaciones externas y/o contratistas que acceden a datos y recursos de información del MTEySS.

Amén de las sanciones disciplinarias o administrativas, y, según corresponda, aquel que causare daño o dolo utilizando información del MTEySS puede incurrir también en responsabilidad civil, patrimonial y/o penal.

Anexo I: Bibliografía y Fuentes de Información

- Modelo de Políticas de SI para la Administración Pública (ICIC),
- Políticas de Seguridad de la Información MTEySS Rev 03, (Res MTEySS 1304/2011)
- ISO/IEC 27001:2013, Requisitos del Sistema de Gestión de Seguridad de la Información ,
- ISO/IEC 27002:2013, Código de práctica para los controles de Seguridad de la información ,
- Norma Para Elaborar Políticas, Procesos y Procedimientos (Res MTEySS 893/2010).

Anexo II: Glosario

Información

Se refiere a toda comunicación o representación de conocimiento en variadas formas: texto, números, gráficos, diagramas cartográficos, narraciones, representaciones audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras u otros.

Datos

A los efectos de documentación y la implementación de las presentes políticas de Seguridad, se considera que *dato* es la unidad de información.

Tipos de Datos

Datos sensibles personales: son los que se refieren a origen racial o étnico, ideología, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual, y se les aplican normas más estrictas para su tratamiento. Estos datos no podrán procesarse ni divulgarse, salvo excepciones concretas (P. ej.: análisis de sangre de la víctima de un accidente). La Dirección Nacional de Protección de Datos Personales –dependiente del Ministerio de Justicia y Derechos Humanos- reglamenta las excepciones, teniendo en cuenta la protección del interés público.

Datos sensibles organizacionales: se refieren a temas propios de una organización, cuya difusión pública aumentaría el riesgo de amenazas a la información. Ejemplo: fórmulas, planes de comercialización, infraestructura informática, etc.

Datos críticos: es toda aquella información cuya indisponibilidad puede afectar el normal funcionamiento del MTEySS.

A los efectos anteriores, toda la información del Organismo deberá estar clasificada, para asignarle un grado de criticidad y un nivel de protección adecuados.

Sistema de Información

Se refiere a un conjunto independiente de recursos de información, organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información

Se refiere al hardware y software utilizados para llevar a cabo gestiones propias de una Organización, a través de computación de datos, telecomunicaciones u otro medio electrónico.

Confidencialidad

Aspecto de la seguridad que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad

Aspecto de la seguridad que salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento de la misma.

Disponibilidad

Aspecto de la seguridad que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad

Aspecto de la seguridad que garantiza el origen de la información, validando el emisor para evitar suplantación de identidades. Busca asegurar la validez de la información en tiempo, forma y distribución.

Auditabilidad

Define que todos los eventos de un sistema de información deben poder ser registrados para su control posterior.

Protección a la duplicación

Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. En un control que impide la grabación de una transacción, para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio

Aspecto de la seguridad que pretende evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad

Se refiere al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta una Organización.

Confiabilidad de la Información

Garantiza que la información generada por un proceso sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones que competen a una Organización.

Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas de una organización, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante el aprovechamiento de una vulnerabilidad, o por un intento de romper los mecanismos de seguridad existentes.

Evaluación de Riesgos

Se refiere a la determinación de amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, así como de estudiar la probabilidad que ocurran, junto con el potencial impacto en la operatoria de una Organización.

Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

Acciones de Tratamiento de Riesgos

- *mitigar o disminuir* los riesgos a un nivel tolerable según las políticas establecidas, mediante aplicación de controles apropiados,
- *aceptar o asumir* los riesgos de manera objetiva y consciente, cuando el nivel de un riesgo es tolerable, o cuando el costo de mitigación es económicamente inviable para el Organismo,
- *evitar* los riesgos, eliminando las acciones que dan origen a la ocurrencia de éstos,
- *transferir* los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguros o proveedores.

Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales. Un control puede ser de naturaleza administrativa, técnica, de gestión, o legal.

Control es también utilizado como sinónimo de salvaguarda o de contramedida.

Gestión de Riesgos

Actividades coordinadas para dirigir y controlar los riesgos que enfrenta una organización.

La gestión de riesgos usualmente incluye: la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

Amenaza

Causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

Vulnerabilidad

Una debilidad de un activo o grupo de activos, que puede ser aprovechada por una amenaza.