Asegurar que los usuarios internos, organizaciones externas y contratistas estén al tanto de las amenazas y riesgos a la seguridad de la información, que conozcan sus derechos y obligaciones, y que estén capacitadas para apoyar la política de seguridad de los datos del MTEySS, en el curso de su labor cotidiana, reduciendo así el riesgo de error humano.

5.2.1 Control: Responsabilidad de las Autoridades

El Responsable de Recursos Humanos, junto con los Responsables Primarios, de Informática y de Seguridad de la Información donde corresponda, verificará que tanto el personal como las organizaciones externas y/o contratistas, donde corresponda, cumplan con las políticas y los procedimientos de seguridad establecidos para la información del MTEySS.

Se deberá observar lo siguiente:

- brindar tener conocimiento adecuado sobre los roles y responsabilidades de seguridad de cada usuario, antes que le sea otorgado el acceso a los recursos de información del MTEySS,
- concientizar sobre las expectativas de seguridad correspondientes a los roles y tareas de cada usuario,
- proporcionar conocimiento sobre las políticas de seguridad del MTEySS,
- verificar el cumplimiento de las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del Organismo y los métodos adecuados de trabajo.

5.2.2 Control: Concientización, formación y capacitación en seguridad de la Información

Todos el personal del MTEySS, cualquiera sea su nivel de contratación, y cuando sea pertinente, las organizaciones externas y contratistas que desempeñen funciones en el Organismo, deben recibir una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del Organismo. Esto comprende lo siguiente:

- requerimientos de seguridad de la información y responsabilidades legales,
- uso correcto de los recursos y activos de información.

5.2.2.1 Responsabilidades y Actores en la Concientización y Capacitación

El Responsable de Recursos Humanos deberá coordinar las acciones de capacitación que surjan de la presente Política.

El material de capacitación deberá ser revisado con una frecuencia anual, como mínimo, para evaluar la pertinencia de su actualización.

El material para las actividades de capacitación será proporcionado por los Responsables de Informática y Seguridad Física, donde corresponda, con la colaboración del Responsable de Seguridad de la Información.

5.2.2.2 Actividades de Inducción y Capacitación

El personal que ingrese al MTEySS deberá recibir material de capacitación, donde se indique el comportamiento esperado en lo que respecta a la seguridad de la información, antes que le sean otorgados los privilegios de acceso a los sistemas que correspondan a sus funciones.

Asimismo, se deberán arbitrar mecanismos para comunicar a todo el personal las eventuales modificaciones o novedades en materia de seguridad, prioritariamente las de carácter crítico.

5.2.3 Control: Proceso disciplinario

En caso de una violación a las Políticas de Seguridad de la Información del MTEySS, el proceso disciplinario deberá ajustarse a lo contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional.

El proceso disciplinario también se puede utilizar como un elemento disuasivo para evitar que los usuarios internos, organizaciones externas y/o contratistas transgredan las políticas y/o cometan cualquier otro incumplimiento de la seguridad.

5.2.4 Control: Compromiso de Confidencialidad y Uso Adecuado de los recursos de información

En tal sentido, como parte de los términos y condiciones de empleo, el personal, cualquiera sea su situación de revista, suscribirá un Compromiso de Confidencialidad y Uso adecuado de los recursos de información del MTEySS.

La gestión de los Compromisos de Confidencialidad deberá ser efectuada por el Responsable de Seguridad de la Información, en colaboración por el Responsable de Informática. La copia firmada del Compromiso debe ser incorporada a los registros y legajos que el área de Recursos Humanos tenga del personal.

5.2.4.1 Aspectos a considerar

Los compromisos de confidencialidad y uso adecuado de los recursos de información contemplarán lo siguiente:

- se notificará en forma fehaciente a los usuarios sobre: sus derechos y obligaciones en lo atinente a la Seguridad de la Información del MTEySS, la protección de activos, la ejecución de procesos y actividades específicas de gestión, la privacidad y protección de datos del Organismo, y las pautas de uso adecuado de los recursos de información,
- se indicará claramente que las actividades de los usuarios, en el ámbito del Organismo, pueden ser objeto de control y monitoreo, en uso del derecho del MTEySS a mantener una adecuada protección a la información y los recursos de su propiedad,
- se respetará el derecho a la privacidad del empleado, donde corresponda,
- indicará claramente que los derechos y obligaciones se extienden más allá de los límites de las sedes del MTEySS y del horario normal de trabajo.

5.2.4.2 Comunicación del Compromiso de Confidencialidad y Uso Adecuado de los Recursos de Información

El Responsable de Recursos Humanos establecerá los mecanismos de divulgación y notificación fehaciente del Compromiso de Confidencialidad y Uso de la información y los recursos Informáticos.

5.2.5 Control: Verificaciones sobre el personal

Los Responsables Primarios, en colaboración con los Responsables de Recursos Humanos y Seguridad de la Información, deberán verificar que el personal que presta tareas en las áreas a su cargo aplique la seguridad en concordancia con las políticas y procedimientos establecidos por el MTEySS.

Se deberá cumplir con lo siguiente:

- verificar que el personal se halle adecuadamente informado de sus roles y responsabilidades sobre la seguridad, antes que se implementen los accesos a los datos y/o los sistemas de información,
- verificar que el personal reciba capacitación y concientización adecuada, en materia de seguridad de la información,
- garantizar que el personal tenga un nivel de conciencia sobre la seguridad acorde con sus roles y responsabilidades dentro del MTEySS,
- garantizar que se cumplan con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del MTEySS,
- mantener las habilidades y calificaciones adecuadas para el personal

5.2.6 Control: Cambio de Funciones o Desplazamientos del Personal del Organismo

Los Responsables Primarios deben informar fehacientemente los casos de cambio de funciones o desplazamientos del personal a otras áreas del MTEySS. Debe comunicarse de estas novedades a los Responsables de Seguridad de la Información, de Informática, de Seguridad Física y de Recursos Humanos, según corresponda.

Se indicarán todas las novedades sobre cambios de función, ubicación física y horarios de trabajo, a los fines de modificar adecuadamente los privilegios de acceso físico y lógico a los recursos de información.

Se considerarán, donde corresponda, aspectos tales como:

- devolución del equipamiento asignado al área saliente,
- asignación de equipamiento en el área entrante, al personal que cambia sus funciones o área de trabajo,
- desplazamiento de equipamiento al personal que cambia de funciones o área de trabajo.

5.3 Categoría: Cese del empleo o cambio de puesto de trabajo

Objetivo

Asegurar que los usuarios empleados, organizaciones externas y/o contratistas, donde corresponda, se desvinculen del MTEySS de una manera ordenada y segura.

5.3.1 Control: Responsabilidades del cese o cambio

Las responsabilidades para realizar la desvinculación deben ser claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori.

Se debe verificar el mantenimiento, dentro de un plazo apropiado, de las responsabilidades contenidas en el compromiso de confidencialidad, así como de los términos y condiciones de empleo, donde corresponda.

5.3.2 Control: Devolución de activos

Tanto el personal como organizaciones externas y/o contratistas, devolverán todos los activos del MTEySS que se hallen en su poder, antes de la finalización fehaciente del vínculo laboral existente con el Organismo, efectuándose los registros formales que correspondan.

Asimismo, todo dato importante para las operaciones, conocido por quienes se hallan en situación de desvinculación, deberá documentarse y transferirse al Organismo.

El Responsable Primario estará a cargo de las gestiones de devolución, con la colaboración de los Responsables de Informática, Seguridad de la Información, Área Administrativa, Recursos Humanos y Seguridad Física, según corresponda.

5.3.3 Control: Retiro de los derechos de acceso

Ante la desvinculación, se deberán quitar los accesos lógicos y privilegios de operación de los activos asociados con los sistemas y servicios de información.

Esta gestión debe estar autorizada por el Responsable Primario, junto con el Responsable de Recursos Humanos, siendo gestionada por el Responsable de Seguridad de la Información, con la implementación por parte del Responsable de Seguridad Informática.

En lo referente al acceso físico, se debe contemplar lo siguiente:

- efectuar la gestión de recuperar llaves y/o tarjetas de identificación,
- efectuar la revocación de claves de acceso físico a instalaciones de procesamiento de la información,

- efectuar la recuperación de cualquier documentación que identifique a la persona como un miembro del MTEySS.

La gestión de revocación del acceso físico debe estar autorizada por el Responsable Primario, junto con el Responsable de Recursos Humanos, e implementada por el Responsable de Seguridad Física.

6. Cláusula: Seguridad Física y Ambiental

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños a la información y a las operaciones del MTEySS. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta:

- perímetros de protección física de los accesos, para facilitar la implementación de controles de acceso físico para las instalaciones de procesamiento de información del MTEySS,
- control ambiental, para garantizar el correcto funcionamiento de los equipos de procesamiento, de forma de minimizar interrupciones en los servicios de información,
- transporte, protección y mantenimiento de equipamiento y documentación.

Objetivo

Los objetivos de esta cláusula son:

- establecer los requerimientos de seguridad que permitan evitar el acceso físico no autorizado a las instalaciones de procesamiento de información del MTEySS,
- establecer las pautas para definir áreas seguras, delimitadas por perímetros de seguridad, donde se ubicarán los equipos de procesamiento de información del MTEySS,
- definir mecanismos y controles adecuados para los perímetros de seguridad, de manera de lograr una protección proporcional a los riesgos que se hayan identificado,
- establecer procedimientos que contemplen traslados de equipamiento fuera de los perímetros de seguridad, cuando ello se haga necesario,
- definir controles para los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento que alberga información del MTEySS,
- proponer medidas para proteger la información que se maneja en las oficinas, en el marco de las labores habituales del personal del MTEySS.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información del MTEySS: instalaciones, equipamiento informático, cableado, medios de almacenamiento y soporte de la información.

Responsabilidad

El Responsable de Seguridad Física, los Responsables Primarios, de Seguridad de la Información y de Informática, según corresponda, establecerán:

- las medidas de seguridad física y ambiental para el resguardo de los activos de información, en función a un análisis de riesgos,
- el control de la implementación de los mecanismos de seguridad física y ambiental,
- el control del cumplimiento de las disposiciones sobre seguridad física y ambiental establecidas.

El Responsable de Seguridad de la Información se ocupará de:

- asistir al Responsable de Seguridad Física en la definición de las medidas de seguridad a implementar en las áreas seguras,
- coordinar la implementación de los mecanismos de seguridad, donde corresponda.

El Responsable de Informática se ocupará de:

- colaborar en la implementación de los mecanismos de seguridad, donde corresponda,
- controlar que los procedimientos de instalación y mantenimiento del equipamiento informátic estén de acuerdo con las especificaciones de los proveedores, tanto dentro como fuera de las instalaciones del MTEySS.

Los Responsables Primarios deberán:

- definir y documentar los niveles de acceso físico del personal del MTEySS a las áreas restringidas que se hallen bajo su responsabilidad. Los Responsables de Seguridad Física, Recursos Humanos, Seguridad de la Información, e Informática, según corresponda, deberán estar informados de esta definición,
- definir y documentar el horario de trabajo del personal a su cargo, informando de ello a los Responsables de Seguridad Física, Recursos Humanos, Seguridad de la Información y de Informática,
- autorizar formalmente al personal a su cargo para que trabaje fuera de las instalaciones del MTEySS, cuando lo crea conveniente, informando a los Responsables de Seguridad Física, Recursos Humanos, Seguridad de la Información y de Informática.

La Unidad de Auditoría Interna revisará los registros de acceso a las áreas protegidas.

Tanto el personal del MTEySS como el de organizaciones externas y/o contratistas que se desempeñen en el ámbito del Organismo, serán responsables por el cumplimiento de la política de pantallas y escritorios limpios, a los fines de la protección de la información relativa al trabajo diario en las oficinas.

Política

6.1 Categoría: Áreas Seguras

Objetivo

Los medios de procesamiento de información del MTEySS deben:

- ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con barreras de seguridad física y controles de ingreso/egreso apropiados,
- estar físicamente protegidos del acceso no autorizado y/o de daños físicos.

Se debe minimizar el riesgo que surja por:

- accesos físicos no autorizados,
- interferencia a la información, provocada por los accesos físicos no autorizados,
- daños a las instalaciones físicas y a la información del MTEySS.

6.1.1 Control: Perímetro de seguridad física

La protección física se llevará a cabo mediante la creación de diversas barreras y/o controles físicos, tanto en las sedes del MTEySS, como en las instalaciones de procesamiento de información.

6.1.1.1 Definición de un perímetro de seguridad física

Un perímetro de seguridad está formado por una barrera tal como: una pared, una puerta de acceso controlados por un dispositivo de autenticación, o un escritorio u oficina de recepción atendidos por personas y/o guardias de seguridad.

El emplazamiento y la fortaleza de cada barrera estarán basados en una evaluación de riesgos. Las especificaciones del perímetro de seguridad serán establecidas por el Responsable de Seguridad Física, con el asesoramiento de los Responsables de Seguridad de la Información y de Informática, donde corresponda.

6.1.1.2 Especificación de controles en los perímetros de seguridad

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

- definir y documentar claramente el perímetro de seguridad,
- ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida,
- verificar la existencia de áreas de recepción, atendidas por guardias de seguridad. Se establecerán procedimientos para registrar cada ingreso y egreso en forma precisa,
- extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación,
- identificar claramente todas las puertas de incendio que se hallen en un perímetro de seguridad, barreras físicas que abarcan desde el piso hasta el techo, a fin de impedir ingresos no autorizados, contaminación ambiental, incendio o inundación,
- instalar puertas ignífugas y cierre automático,

6.1.2 Control: Controles físicos de entrada

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico.

Dichos controles serán determinados por el Responsable Primario que corresponda, e implementado por el Responsable de Seguridad Física, con la colaboración de los Responsables de Seguridad de la Información y de Informática, según corresponda.

6.1.2.1 Características de los controles físicos

Los controles de acceso físico deberán considerar los siguientes aspectos básicos:

- señalamiento discreto. La señalización para el acceso a las áreas protegidas deber ser discreta, ofreciendo una indicación mínima de su propósito y evitando los signos obvios, tanto en la periferia como en el interior,
- restricción de acceso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados,
- personal de vigilancia y protección física a quienes se desempeñen en áreas seguras,
- registro de las visitas. Se deberá registrar la fecha y horario de ingreso y egreso del visitante, el propósito de la visita y qué funcionario lo atenderá. Se lo instruirá, además, sobre los requerimientos de seguridad del área y procedimientos de emergencia,
- autenticación y validación de accesos. Se recomiendan métodos de autenticación de factor múltiple, para validar todos los accesos, p. ej.: utilización de tarjetas de identificación con ingreso de contraseña y/o personal de vigilancia y sistema de ingreso/egreso con habilitación por tarjeta magnética,
- uso de una identificación unívoca. Dicha identificación deberá ser visible, debiendo distinguirse entre el personal del MTEySS y las visitas (proveedores, consultores externos, etc.),
- escolta de visitas o personas ajenas al MTEySS. Todo ajeno que deba ingresar a un área protegida será recibido y escoltado por personal autorizado. La escolta también debe verificarse cuando el visitante se retire del área segura,
- verificación de personas. Se instruirá al personal de las áreas protegidas acerca de interrogar a desconocidos no escoltados por personal autorizado, a quien no exhiba una identificación visible, o quien no disponga de acceso físico autorizado,
- verificación de paquetes y/o pertenencias. Se inspeccionará el contenido de paquetes, portafolios y carteras, según se amerite, del ingreso de las personas a los edificios del MTEySS y/o a áreas protegidas,

- actualización de derechos de acceso a las áreas protegidas. Donde corresponda, el Responsable Primario verificará y actualizará los accesos a las áreas. Dicha información será comunicada a los Responsables de Seguridad Física, de Seguridad de la Información y de Informática, donde corresponda,
- auditoría de los registros de acceso. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información,
- controles de seguridad física en instalaciones en la nube. En caso de almacenar y/o procesar datos en la nube (*cloud computing*), los contratos considerarán la verificación de la protección física de las instalaciones del proveedor de los servicios.

6.1.3 Control: Seguridad de oficinas, despachos e instalaciones

6.1.3.1 Características de las áreas seguras

Un área segura o protegida es una oficina o grupo de oficinas, rodeada por un perímetro de seguridad. En algunos casos, en un área segura pueden ser necesarias barreras adicionales, con diferentes requerimientos de seguridad, p. ej.: área de almacenamiento para certificados de firma digital, dentro de un centro de procesamiento informático.

Los siguientes son aspectos a ser tenidos en cuenta en las áreas seguras del MTEySS:

- deben implementarse sistemas de vigilancia y detección de intrusos (cámaras, detectores de proximidad, etc.), a fin de evitar el riesgo por irrupción,
- la ubicación debe ser de difícil acceso,
- las puertas y ventanas deben tener protección externa. Las mismas permanecerán cerradas, especialmente cuando no se verifique la presencia de personal de vigilancia,
- los centros de cómputo no deben tener ventanas,
- las paredes externas del área deben ser sólidas,
- el equipamiento de soporte, (p. ej.: impresoras, fotocopiadoras, máquinas de fax), se ubicará dentro del área protegida para evitar accesos no autorizados que comprometan a la información,
- el personal de operaciones debe trabajar en áreas seguras separadas de los centros de cómputo,
- se deben implementar sistemas de detección y eliminación de incendio y/o filtraciones de agua, donde corresponda,
- se debe restringir la publicación de números de teléfono pertenecientes a recintos de procesamiento de información sensible y/o crítica,
- se deben implementar sistemas de control de condiciones ambientales e iluminación de emergencia,
- debe requerirse la presencia de personal para controlar el acceso físico a las áreas seguras,
- se deben verificar, en forma periódica, las condiciones ambientales y el funcionamiento de los controles. El Responsable de Seguridad Física efectuará dichas verificaciones, informando a los Responsables Primarios, de Recursos Humanos, de Seguridad de la Información y de Informática, donde corresponda,
- se deberán instalar pararrayos, tanto en las instalaciones seguras como en todos los edificios del MTEySS Asimismo, se debe disponer de filtros de protección contra descargas estáticas y rayos, sobre todas las líneas de ingreso de energía y comunicaciones,
- se deben implementar, donde corresponda, sistemas de alimentación eléctrica ininterrumpida,

- en los casos de contratación de servicios de información en la nube (*cloud computing*),, las instalaciones físicas del proveedor deben tener protecciones iguales o mayores que las existentes en el MTEySS.

6.1.3.2 Áreas seguras del MTEySS

Se definen como áreas seguras del MTEySS a las siguientes:

- oficinas de autoridades,
- áreas de biblioteca, archivos físicos y de guarda de expedientes,
- áreas de gestión de sumarios administrativos y expedientes legales,
- áreas de operación de sistemas sustantivos,
- centros de cómputo y áreas de operación de la infraestructura de TICs,
- áreas de desarrollo de sistemas informáticos,
- áreas de control de vigilancia, gestión de seguridad informática y auditoría,
- zonas de comando y distribución de energía eléctrica,
- instalaciones de aire acondicionado centralizado,
- instalaciones de procesamiento o almacenamiento de información del MTEySS administradas por contratistas, p. ej.: servicios informáticos en la nube (*cloud computing*).
- instalaciones de equipamiento de comunicaciones.

6.1.3.3 Registro de las áreas seguras del MTEySS

El Responsable de Seguridad Física deberá llevar un registro actualizado de las áreas seguras, así como de los controles implementados en las mismas. Tal información será compartida con los Responsables Primarios que corresponda, así como con los Responsables de Recursos Humanos, de Seguridad de la Información y de Informática.

El registro debe contener, como mínimo, la siguiente información:

- identificación del área segura: edificio, dependencia a la que está asignada, Responsable Primario a cargo de la misma,
- principales elementos a proteger,
- mecanismos y/o procedimientos de protección física implementados en el área.

6.1.4 Control: Protección contra amenazas externas y de origen ambiental

Se deben definir e implementar protecciones físicas para mitigar riesgos por incendios, inundaciones, terremotos, explosiones, disturbios civiles, manifestaciones, acoso al personal y toda otra forma de amenaza, natural o humana.

Para ello, se debe efectuar una evaluación de riesgos para establecer las acciones de prevención y/o solución que se requieran, ante un incidente.

Debe tenerse en cuenta la posibilidad de amenazas provocadas por inmuebles vecinos, p. ej.: fuego en un edificio contiguo, filtraciones de agua en medianeras, techo o pisos, o una explosión de gas en la calle.

El Responsable de Seguridad Física, junto con el Responsable de Seguridad de la Información, el Responsable de Informática y los Responsables Primarios a cargo, deberá considerar los siguientes aspectos:

- los materiales peligrosos y combustibles, así como los suministros a granel y la papelería, deben almacenarse a una distancia considerable por fuera del área asegurada,
- los medios de resguardo deben ubicarse a una distancia considerable, para evitar pérdidas en caso que una contingencia severa o un desastre impacten sobre el área segura,

- las instalaciones de contingencia y/o continuidad de la gestión deben hallarse a una distancia mayor a 200 metros del centro de cómputos principal,
- los equipos de detección, las alarmas y los dispositivos de tratamiento de incendios deben ubicarse adecuadamente,
- se establecerán planes de administración de contingencias, los que se ensayarán y actualizarán en forma periódica,
- se elaborarán planes de evacuación, adecuados a las distintas áreas físicas.

6.1.5 Control: Trabajo en áreas seguras

Para quienes se desempeñan en áreas protegidas se establecen los siguientes controles y pautas adicionales:

- las actividades que se desarrollan en las áreas seguras deben estar autorizadas y registradas formalmente,
- las actividades que se llevan a cabo en un área protegida sólo serán conocidas por aquellos que lo requieran, para el desarrollo de sus funciones,
- las actividades que llevan a cabo contratistas en las áreas protegidas estarán supervisadas en forma estricta,
- las áreas desocupadas deberán estar bloqueadas al acceso físico, y serán inspeccionadas periódicamente por los Responsables Primarios a cargo de las mismas,
- se debe disponer de un detalle de horarios de trabajo y/o turnos del personal que presta funciones en las áreas protegidas. El mismo será confeccionado por los Responsables Primarios pertinentes, y difundido a los responsables de Seguridad Física, Recursos Humanos, Seguridad de la Información e Informática,
- el personal de servicio (contratistas de soporte, personal de limpieza) tendrá acceso limitado, y sólo cuando sea autorizado por el Responsable Primario que corresponda. Este acceso deberá estar registrado en cada caso, y será supervisado por el personal pertinente,
- pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, dentro de un mismo perímetro de protección. Esto se aplica, por ejemplo, al centro de cómputos, las áreas de administración del mismo, y toda zona donde se desarrollen sistemas informáticos, o se procese información sensible,
- en el caso de servicios en la nube, se verificarán las tareas de administración y soporte que efectúe el contratista, en lo atinente a las protecciones físicas de la instalación,
- el ingreso a las áreas seguras con equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información estará prohibido. Las excepciones estarán formalmente autorizadas por el Responsable Primario a cargo de dicha área y/o por el Responsable de Seguridad Física y/o los Responsables de Seguridad de la Información y de Informática, donde sea pertinente,
- se prohibirá comer, beber y fumar dentro de las instalaciones de procesamiento de la información, centros de cómputo y/o salas de comunicaciones.

6.1.6 Control: Áreas de acceso público, de carga y descarga

Las áreas de depósito y de acceso público estarán totalmente separadas de las instalaciones de procesamiento y operación de los datos del MTEySS.

6.1.6.1 Áreas de Depósito

Se establecerán las siguientes pautas:

- permitir el acceso a las áreas de depósito a personal previamente autorizado e identificado adecuadamente,

- los requisitos de los perímetros de seguridad y las condiciones ambientales serán las adecuadas al material que se esté almacenando, p. ej: accesos restringidos y condiciones de temperatura y humedad ambiente adecuadas para la guarda de medios de almacenamiento magnético/óptico,
- el servicio de vigilancia debe ser de 7x24x365, especialmente donde se almacene información sensible,
- diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio,
- proteger todas las puertas exteriores del depósito cuando se abre la puerta interna, p. ej.: con sistemas de puerta-trampa,
- se efectuarán inspecciones periódicas, especialmente en depósitos no atendidos por personas físicas, a efectos de detectar variaciones en las condiciones ambientales y de seguridad,
- implementar procedimientos de inspección del material entrante.

6.1.6.2 Áreas de acceso al público

Se establecerán las siguientes pautas:

- las oficinas de atención al público estarán abiertas en los horarios habilitados a tal efecto. Fuera de ese horario, las áreas permanecerán cerradas, y el acceso estará habilitado para el personal autorizado, exclusivamente,
- el servicio de vigilancia se reforzará durante el horario de atención al público,
- se habilitará un servicio de circuito cerrado de TV, para reforzar la labor de la vigilancia física,
- el almacenamiento de información debe hallarse fuera de las áreas de atención al público,
- los puestos de trabajo informático deben disponer de mecanismos antirrobo.

6.2 Categoría: Seguridad de los equipos

Objetivo

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de la operatoria del MTEySS. El equipamiento informático utilizado como puesto de trabajo debe estar protegido contra amenazas físicas y ambientales.

6.2.1 Control: emplazamiento y protección de equipos

Se efectuará un análisis de riesgos para ayudar a determinar la ubicación física del equipamiento informático. Se deben tener en cuenta los siguientes factores:

- ubicar el equipamiento en sitios donde se pueda disponer de un control de accesos adecuado,
- las instalaciones de procesamiento y almacenamiento de información se hallarán en sitios donde se mantenga el acceso controlado,
- el equipamiento informático, cualquiera sea su tipo, debe instalarse en sitios donde se minimicen los riesgos por factores atmosféricos (p. ej.: tormentas eléctricas e inundaciones), siniestros (p. ej.: incendios, derrumbes o escapes de gas), factores ambientales (p. ej.: humo polvo, efectos químicos, descargas eléctricas o vibraciones), problemas de suministro eléctrico, temperatura y/o humedad ambiental,
- el impacto de las amenazas citadas anteriormente, si éstas se materializan en edificios vecinos a las sedes del MTEySS.

6.2.2 Control: Instalaciones de Suministro

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

Los Responsables de Seguridad de la Información y de Informática, junto con los Responsables Primarios pertinentes, efectuará un análisis de riesgo sobre los sistemas informáticos.

De acuerdo con los resultados del análisis mencionado, tanto el Responsable de Seguridad Física, como el Responsable de Informática, establecerán planes para la implementación de las pautas de seguridad para el suministro eléctrico, garantizando así la continuidad del servicio en la gestión del MTEySS.

Para asegurar el suministro de energía, se contemplarán las siguientes medidas de control:

- implementar sistemas de alimentación eléctrica controlada y regulada a los valores especificados por las normas argentinas,
- en las salas donde se ubica el equipamiento informático, ubicar tableros de comando e interruptores de emergencia en lugares estratégicos, para facilitar una operación rápida en caso de situaciones críticas,
- instalar sistemas de iluminación de emergencia en caso de producirse una falla en el suministro principal,
- implementar protecciones contra descargas eléctricas, en todos los edificios y líneas de comunicaciones externas,
- disponer de múltiples entradas de alimentación, para evitar un único punto de falla en el suministro,
- instalar múltiples tomas de conexión, distribuidas estratégica y funcionalmente en los recintos de instalación,
- instalar sistemas de energía interrumpible (UPS) para asegurar la operación continua del equipamiento que sustenta las operaciones críticas del MTEySS,
- instalar grupos electrógenos, para contemplar casos de corte de energía prolongado,
- implementar procedimientos de inspección y ensayo sobre los equipos de UPS y grupos electrógenos. Estos procedimientos se deberán llevar a cabo en forma periódica, y deberán garantizar un adecuado funcionamiento y una autonomía acorde a lo requerido. Se deben realizar las siguientes verificaciones: estado de carga de combustible y tiempo de puesta en régimen de los grupos electrógenos, carga de las baterías de las UPS, etc.,
- implementar procedimientos de encendido y apagado de equipamiento informático, según las especificaciones de los fabricantes.

6.2.3 Control: Seguridad del cableado

Deberá protegerse el cableado de energía eléctrica y de comunicaciones de datos contra intercepción o daño, en las instalaciones de procesamiento de la información del MTEySS.

El Responsable de Seguridad Física, junto a los Responsables de Seguridad de la Información y de Informática, definirá y verificará el cumplimiento de las pautas de seguridad para el cableado eléctrico y de comunicaciones.

Se llevarán a cabo las siguientes acciones:

- cumplir con los requisitos técnicos vigentes, en cuanto a las normativas referidas a instalaciones eléctricas e informáticas,
- utilizar piso ductos o conductos embutidos en la pared, siempre que sea posible,
- mantener el cableado eléctrico en conductos separados del correspondiente a datos, para minimizar o evitar interferencias,

- verificar las conexiones a tierra que correspondan,
- verificar los blindajes de conductos.

6.2.4 Control: Mantenimiento de los equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsable de Informática quien mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo,
- establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento,
- registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado,
- registrar el retiro de equipamiento de la sede del Organismo para su mantenimiento,
- eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

6.2.5 Control: Seguridad de los equipos fuera de las instalaciones del MTEySS

El uso de equipamiento informático fuera del ámbito del MTEySS será autorizado por el Responsable Primario, debiendo informar a los Responsables de Administración, Seguridad de la Información, Informática y Seguridad Física.

Previo a la autorización, se efectuará un análisis de los riesgos, suscitados por las condiciones físicas y la infraestructura tecnológica existentes en el ámbito de la instalación del equipamiento, además de daño, robo o intercepción.

Se deberán tener en cuenta los siguientes aspectos:

- la seguridad física provista debe ser equivalente a la suministrada dentro del ámbito del MTEySS para un propósito similar, aun cuando las condiciones ambientales y físicas varíen considerablemente entre edificios,
- se respetarán permanentemente los requisitos de instalación establecidos por el proveedor del equipamiento informático. Se proporcionará, asimismo, una adecuada cobertura de seguro, fuera del ámbito del MTEySS, cuando sea pertinente,
- en caso de operar con información sensible o crítica, el Responsable Primario debe declararlo taxativamente al efectuarse el análisis de riesgos, a fin de determinar si deben reforzarse los controles de seguridad existentes.

6.2.6 Control: Reutilización o retiro seguro de activos

La información puede verse comprometida por una desafectación o una reutilización descuidada de los activos de información.

Se efectuará una evaluación de riesgos para determinar el tratamiento a seguir con los medios que contienen información del MTEySS. Se determinará, p. ej., si los medios de almacenamiento dañados que contienen datos sensibles deben ser destruidos, reparados o desechados. También deben efectuarse consideraciones sobre el impacto en el medio ambiente.

El Responsable de Seguridad de la Información definirá y verificará el empleo de los mecanismos para la reutilización, baja y/o desafectación de activos de información, siendo éstos implementados por Responsables Primarios, de Informática, Seguridad Física y/o Administración, donde corresponda.

Se deben utilizar los siguientes métodos y/o mecanismos:

- en computadoras, tabletas, teléfonos inteligentes netbooks y/o notebooks, cuando se los reutilice, formateo de bajo nivel de discos rígidos, donde corresponda, y reinstalación limpia,

- en discos rígidos, formateo de bajo nivel, sobre escritura segura, procedimientos de desmagnetización y/o destrucción física, donde corresponda,
- en dispositivos USB, borrado, formateo lógico y/o destrucción física,
- en medios de almacenamiento magnético/ópticos (CDs, DVDs, diskettes, cartuchos de cinta), destrucción física,
- en datos bajo soporte en papel, utilizar destructoras.

6.2.7 Control: Retiro de materiales propiedad de la empresa

Queda prohibido retirar equipamiento, información y software del MTEySS sin la correspondiente autorización formal. Dicha autorización será emitida por el Responsable Primario a cargo del bien, con la comunicación a los Responsables de Administración, Seguridad Física, Seguridad de la Información e Informática, según corresponda.

El Responsable de Administración, con la colaboración de los Responsables Primarios, de Seguridad Física, de Informática, de Seguridad de la Información y Unidad de Auditoría Interna, donde corresponda, efectuará verificaciones periódicas, sin aviso previo, a fin de detectar anomalías en los retiros de bienes del MTEySS.

El Responsable de Recursos Humanos comunicará al personal, organizaciones externas y contratistas, sobre la realización de tales verificaciones, en línea con los procedimientos establecidos por la normativa administrativa y legal vigente.

6.2.8 Control: Políticas de Escritorios y Pantallas Limpias

6.2.8.1 Política de Escritorios Limpios

Se adopta una política de escritorios limpios, a los fines de proteger documentos en papel, dispositivos móviles y de almacenamiento removible, a fin de reducir riesgos de acceso no autorizado, pérdidas y/o daño a la información del MTEySS.

Los Responsables Primarios establecerán un registro de las contraseñas de acceso físico, disponiendo asimismo de copias de las llaves de seguridad utilizadas en los sectores a su cargo.

Las condiciones de guarda de documentación y/o medios removibles estarán definidas por los Responsables Primarios, con la colaboración de los Responsables de Informática, Seguridad de la Información, Seguridad Física y Administración, donde corresponda.

La política de escritorio limpio se aplicará tanto durante el horario normal de trabajo como fuera del mismo.

Se tendrán en cuenta los siguientes lineamientos:

- proteger los puntos de recepción y envío de correo postal y máquinas de fax no atendidas, donde corresponda,
- registrar el uso de fotocopiadoras, y bloquearlas fuera del horario normal de trabajo,
- almacenar bajo llave medios informáticos removibles que contengan información sensible, cuando éstos no sean utilizados, y especialmente fuera del horario laboral,
- documentos que contengan información sensible o crítica del MTEySS deben encontrarse en sobres cerrados y bajo llave, cuando no estén siendo utilizados,
- utilizar cajas fuertes o gabinetes con características ignífugas y robustez física adecuada, para la guarda de documentos y/o medios removibles,
- contratar servicios de guarda externa, donde corresponda, a los efectos de almacenar en condiciones seguras tanto documentos como medios removibles que contengan información crítica,
- mantener un registro de accesos a la información guardada, con una justificación en cada caso sobre los motivos para tales acciones

6.2.8.2 Política de Pantallas Limpias

Se implementará la política de pantalla limpia sobre los puestos de trabajo informático y servidores de red, con el propósito de reducir riesgos de acceso lógico no autorizado, pérdidas y/o daños sobre de la información.

6.2.8.3 Responsabilidades y alcance

El Responsable de Seguridad de la Información definirá y verificará el cumplimiento de la política de pantalla limpia en puestos de trabajo, servidores de red, dispositivos móviles, equipamiento de comunicaciones, impresoras y/o máquinas de fax, donde corresponda.

El Responsable de Informática implementará los controles establecidos.

Esta política se extenderá a los equipos informáticos personales que se conecten a la red y recursos informáticos del MTEySS.

6.2.8.4 Controles a implementar

Deben observarse los siguientes aspectos:

- desconexión y/o bloqueo automático de puestos de trabajo, computadoras personales, impresoras de red y dispositivos móviles, cuando éstos queden desatendidos y/ o fuera de uso. A tal efecto, pueden emplearse mecanismos tales como protectores de pantalla activados por contraseña,
- retiro inmediato de trabajos de impresión enviados a impresoras de red, especialmente cuando éstos contengan información sensible,
- instalación de impresoras locales a puestos de trabajo donde se procese o gestione información crítica o confidencial.

6.2.8.5 Concientización al Usuario y Contratistas

Los Responsables Primarios, con la colaboración de los Responsables de Seguridad de la Información, de Informática y de Capacitación, concientizarán a los usuarios y contratistas sobre las políticas de pantalla limpia a aplicar en los ámbitos que corresponda.

Se requerirá, además, la cooperación de los usuarios para impedir accesos no autorizados, estableciéndose un adecuado nivel de eficacia en la seguridad.

Se deben tener en cuenta los siguientes lineamientos:

- no dejar los puestos de trabajo en forma desatendida, sobre todo en lugares públicos,
- transportar los equipos portables como equipaje de mano, en forma discreta, de ser posible,
- cerrar o bloquear las sesiones de red cuando el usuario se retire de su ámbito de trabajo El protector de pantalla, protegido con contraseña, no podrá deshabilitarse,
- propender a que los equipos personales o de terceros dispongan de una adecuada póliza de seguro.

7. Cláusula: Gestión de Comunicaciones y Operaciones

Generalidades

Los sistemas de información del MTEySS se hallan comunicados entre sí, tanto dentro de la red de datos internas como hacia/desde el mundo de internet. Es necesario, por ende, definir e implementar mecanismos de seguridad en todo intercambio de datos que tenga lugar.

La transferencia de datos debe estar controlada, de manera de garantizar los requisitos de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales. En tal sentido, se verificará una adecuada y eficiente interconexión entre los distintos equipos que conforman la red de datos del MTEySS.

Los controles, deberán garantizar, el funcionamiento correcto y seguro de los procesos que dan apoyo a la gestión del MTEySS.

Se implementarán controles preventivos, para evitar la ocurrencia de amenazas tales como la proliferación de software malicioso, virus, troyanos, robo de identidad y correo no deseado, entre otros.

En lo referente a operaciones, se efectuará una segregación de funciones adecuada, a fin de reducir el riesgo de negligencias y/o manipulación indebida de los sistemas informáticos. En tal sentido, los ambientes de procesamiento informático estarán separados en Desarrollo, Prueba y Producción.

Los procedimientos deberán garantizar la calidad de la información procesada en el ámbito productivo, a fin de minimizar los riesgos de incidentes por manipulación indebida de los datos del MTEySS.

Objetivo

Son objetivos de la presente cláusula:

- garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones,
- establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones para la respuesta a incidentes y separación de funciones.

Alcance

Se hallan alcanzadas todas las instalaciones y las personas involucradas en el procesamiento y la transmisión de información del MTEySS.

Responsabilidad

El Responsable de Seguridad de la información tendrá a su cargo, entre otros aspectos:

- evaluar el cumplimiento de los procedimientos de acceso a los ambientes informáticos,
- colaborar en la definición de procedimientos para la gestión segura –incluyendo la eliminación de datos- de medios informáticos de almacenamiento,
- definir procedimientos para el control de cambios a los procesos operativos, los sistemas y las instalaciones de procesamiento de información, de manera que estos refuercen la seguridad de la información,
- evaluar y verificar los mecanismos de distribución y difusión de información dentro del Organismo, p. ej.: uso del correo electrónico,
- colaborar en la definición de controles para garantizar la seguridad de los datos y los servicios conectados en los ambientes informáticos, las redes del MTEySS y las conexiones a Internet,
- definir y verificar el cumplimiento de aspectos de seguridad para las aplicaciones de Gobierno Electrónico,

- definir procedimientos para el manejo de incidentes de seguridad de la información,
- colaborar en la definición de controles para la detección y prevención contra el acceso lógico no autorizado y software malicioso,
- colaborar en el desarrollo de procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios, con los Responsables de Capacitación y de Informática, donde corresponda,
- verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable de Informática tendrá a su cargo, entre otros:

- implementar procedimientos para el control de cambios a los procesos operativos, los sistemas y las instalaciones de procesamiento informático, asignando las responsabilidades pertinentes, y analizando el posible impacto sobre la infraestructura existente,
- implementar controles de existencia de documentación autorizada, relacionada con los procedimientos de comunicaciones y operaciones,
- implementar y administrar los mecanismos que permitan la segregación de los ambientes informáticos requeridos para el desarrollo, la prueba y la operación de la información,
- implementar procedimientos para la implementación y el control de cambios en los ambientes informáticos, ,
- implementar controles de seguridad en todas las aplicaciones informáticas, especialmente en las relacionadas con Gobierno Electrónico,
- implementar controles con respecto al uso del correo electrónico corporativo,
- implementar mecanismos informáticos para la distribución segura de la información, a través de la red de datos del MTEySS y las conexiones a Internet,
- implementar controles para el uso de dispositivos móviles, de manera de restringir la salida de información por medios no autorizados,
- implementar controles para la detección y prevención contra el acceso lógico no autorizado y software malicioso,
- implementar procedimientos para la gestión –incluyendo la eliminación segura de datos- de medios informáticos de almacenamiento,
- colaborar en el desarrollo de procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios, con los Responsables de Capacitación y de Seguridad de la Información, donde corresponda,
- monitorear las necesidades de capacidad de los sistemas, proyectando las demandas futuras, a fin de prevenir potenciales amenazas a la seguridad de sistemas o servicios al usuario,
- controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración,
- implementar controles para la gestión segura de medios de almacenamiento electrónico,
- asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión,
- implementar procedimientos para el manejo de incidentes de seguridad informática,
- implementar procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones,
- implementar medidas preventivas y/o correctivas por fallas e incidentes en los ambientes de procesamiento informático y los sistemas de comunicaciones,

El Responsable de Seguridad de la información, junto con los Responsables de Informática y del Área Legal, deberá evaluar los contratos y acuerdos con Responsables Primarios, organizaciones externas y/o contratistas, según corresponda, para garantizar la incorporación de requisitos atinentes a la seguridad de la información involucrada en la gestión de accesos, productos y/o servicios no informáticos

Los Responsables Primarios, con la colaboración de los Responsables de Seguridad de la Información y de Informática, establecerán los procedimientos para la operación normal, así como la reanudación y/o las correcciones por fallas.

Los Responsables Primarios, con la colaboración de los Responsables de Seguridad de la Información, de Informática, Seguridad Física y Administración, donde corresponda, determinarán los requerimientos de guarda de la información por la cual son responsables.

Asimismo, cada Responsable Primario deberá aprobar los servicios de mensajería a emplear para el transporte la información, cuando se requiera, de acuerdo a su nivel de criticidad.

El Comité de Seguridad de la Información colaborará en la definición de los procedimientos y políticas que garanticen la mayor protección a los datos del MTEySS.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, revisará las actividades que no hayan sido posibles segregar, así como los registros de actividad del personal operativo.

Política

7.1 Categoría: Procedimientos y Responsabilidades Operativas

Objetivo

Asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se deben establecer las responsabilidades y el desarrollo de procedimientos para la gestión y operación de todos los recursos de información del MTEySS.

7.1.1 Control: Documentación de los Procedimientos Operativos

Los procedimientos para la operación de los sistemas informáticos serán documentados y actualizados por el Responsable de Informática, en colaboración con el Responsable de Seguridad Informática, y con comunicación a los Responsables Primarios que corresponda.

7.1.1.1 Instrucciones para la operación de los sistemas

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas,
- métodos para procesar y gestionar la información,
- manejo de errores y condiciones de excepción,
- restricciones en el uso de utilitarios del sistema,
- personal de soporte a contactar en caso de problemas operativos o técnicas imprevistas,
- instrucciones especiales para la gestión de las salidas de información, p. ej. uso de papelería especial, distribución de salidas confidenciales y eliminación segura de salidas de tareas fallidas,
- procedimientos de reinicio y recuperación en caso de fallas en el sistema.

7.1.1.2 Procedimientos adicionales

Se preparará, asimismo, documentación sobre procedimientos referidos a las siguientes actividades:

- instalación y mantenimiento de las plataformas de procesamiento y puestos de operación,
- instalación y mantenimiento del equipamiento de comunicaciones,
- monitoreo del procesamiento y las comunicaciones,
- fases de inicio y finalización de la ejecución de los sistemas,
- programación y ejecución de procesos,
- gestión de servicios,
- resguardo de información,
- gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones,
- reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones,
- utilización del correo electrónico.

7.1.2 Control: Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en los ambientes informáticos y de comunicaciones, luego de haber efectuado evaluaciones previas sobre los aspectos técnicos y de seguridad.

El Responsable de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de la información del MTEySS.

El Responsable de Informática evaluará el posible impacto operativo de los cambios previstos, verificando además su correcta implementación.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

- identificación y registro de cambios significativos,
- evaluación del posible impacto de dichos cambios,
- aprobación formal de los cambios propuestos,
- planificación del proceso de cambio,
- prueba del nuevo escenario,
- comunicación de los detalles del cambio a los Responsables Primarios y demás actores pertinentes,
- implementación de un registro de auditoría que contenga toda la información relevante de los cambios llevados a cabo,
- identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

7.1.3 Control: Separación de Funciones

Se deben tomar recaudos para que en las áreas de responsabilidad única no se realicen actividades sin que haya un monitoreo, verificando la independencia entre el inicio de un evento y su autorización.

Se separará la gestión y la ejecución de tareas o áreas de responsabilidad, a fin de reducir el riesgo por:

- operaciones no autorizadas,
- mal uso de la información o los servicios,
- definición deficiente de la interdependencia en la ejecución de procesos críticos.

7.1.3.1 Pautas para la separación de funciones

Se debe garantizar el cumplimiento de lo siguiente:

- asegurar la independencia de las funciones de auditoría y de seguridad, con respecto a las operaciones,
- separar actividades que puedan presentar riesgo de connivencia para defraudar, p. ej.: procesar una orden de compra y verificar que la mercadería fue recibida,
- *establecer controles duales o por oposición, de forma que se reduzca el riesgo de prácticas* deshonestas,

7.1.3.2 Controles compensatorios

En caso de no poder efectuar una separación completa de funciones, se implementarán controles tales como:

- monitoreo de las actividades,
- registros de auditoría y control periódico de los mismos,
- supervisión por parte de la Unidad de Auditoría Interna, o de quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas,
- justificación formal y documentada por la cual no fue posible efectuar la segregación de funciones.
- accesos restringidos a operadores y programadores autorizados para cada ambiente de trabajo.

7.1.4 Control: Separación entre las Instalaciones de Desarrollo, Prueba, Homologación y Producción

Los ambientes de desarrollo, prueba, homologación y producción, siempre que sea posible, estarán separados preferentemente en forma física. Se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo, considerando otros estados intermedios como el de pruebas, homologación y/u otros.

Las reglas de transferencia de información y acceso entre los distintos ambientes estarán definidas por el Responsable de Seguridad de la Información, con la colaboración de cada Responsable Primario, donde corresponda, e implementadas por el Responsable de Informática.

7.1.4.1 Infraestructura básica

En el MTEySS se dispondrá como mínimo de los siguientes ambientes:

- un ambiente para el desarrollo de los sistemas. Es un ambiente inestable.
- un ambiente para probar los sistemas recién desarrollados. Es un ambiente inestable,
- un ambiente de homologación (o *staging*), para validar las características (funcionalidad, seguridad, rendimiento, integración y otras) de los sistemas provenientes del ambiente de prueba, antes de su pasaje a producción. Es un ambiente estable,
- un ambiente de producción, para el proceso de los datos del MTEySS.

7.1.4.2 Perfiles operativos de los ambientes

Los principales perfiles de las personas que operan los diferentes ambientes, son:

- *implementador, mantiene el control de gestión sobre los ambientes, y sus funciones son:*
  - actualizar y/o distribuir, con exclusividad, bibliotecas de programas fuente y rutinas ejecutables,
  - administrar el almacenamiento de las bibliotecas de programas,

- verificar la disponibilidad de documentación relativa a la puesta en marcha de los aplicativos, junto con el testeador,
- implementar los pasajes de ambientes de prueba a producción,
- mantener la infraestructura de soporte de los ambientes.

- *testeador funcional*, cuyo desempeño se centra en el ambiente de pruebas, y sus funciones son:
  - realizar las verificaciones de los sistemas con un lote de datos de pruebas,
  - verificar la pertinencia de la documentación existente de los sistemas que pasarán a homologación, para su validación final,
- *testeador de seguridad*, cuyo desempeño se centra en el ambiente de homologación, y sus funciones son:
  - realizar las verificaciones de seguridad en el código de los sistemas,

7.1.4.3 Características operativas del ambiente de desarrollo

En este entorno se desarrollan los programas fuente y/o rutinas ejecutables, además de almacenarse toda la información relacionada con el análisis y diseño de los sistemas.

Algunas características del ambiente:

- se debe disponer de un sistema de gestión de versiones (versionador),
- se definen los perfiles de Analista, Programador y/o Desarrollador, quienes tienen control total en el entorno,
- se establece, además, el perfil del Administrador de bibliotecas de programas fuente, quien tiene control sobre el versionador,
- en el ambiente se crean o modifican programas fuente y/o rutinas ejecutables, registrándose lo actuado en el sistema de control de versiones,
- para el desarrollo, se implementa un lote de datos que contendrá información apócrifa. Las bases mantendrán, donde sea pertinente, el mismo modelo de datos de los sistemas existentes en producción. El Administrador de Bases de Datos de la infraestructura informática verificará el cumplimiento de este punto,
- cuando se estima que el desarrollo ha finalizado, se autoriza el pasaje al ambiente de pruebas. En dicha operatoria debe adjuntarse toda la documentación del sistema en cuestión,

7.1.4.4 Características operativas del ambiente de pruebas

En este entorno se efectúa un testeo de los sistemas emitidos desde el ambiente de desarrollo.

Algunas características de este ambiente:

- el testeador recibe el programa y la documentación respectiva, la que es verificada, realizando luego una prueba general con un lote de datos preparado para tal efecto,
- si no se encuentran errores, el testeador pasa el sistema al implementador, para iniciar el proceso de pasaje a homologación,
- en caso de no cumplirse las verificaciones, el testeador vuelve el ciclo hacia atrás, devolviendo el programa al desarrollador, junto con un detalle de observaciones y hallazgos.

7.1.4.5 Características operativas del ambiente de homologación

Homologación es el ambiente para pruebas de aceptación por parte del usuario final, antes que un sistema o una actualización pase a producción. Es también el ambiente recomendado para la integración de aplicaciones.

Se trata de un entorno similar al ambiente de operaciones, conteniendo siempre la versión actual del sistema, o la próxima a implementarse. En este ambiente accederá el implementador y/o el equipo de testeo, además de los usuarios autorizados, según corresponda.

- se efectúan validaciones junto con el usuario final,
- se verifica si las rutinas de seguridad programadas se corresponden con las especificaciones,
- se verifican las interfaces y la integración especificada con otros sistemas interdependientes.

7.1.4.6 Características operativas del ambiente de producción

En este entorno se ejecutan los sistemas informáticos, y se procesa la información pertinente a las operaciones del Organismo.

Las características principales de este ambiente son:

- los programas fuente que se hallan certificados para el ambiente se almacenan en un repositorio de fuentes de producción,
- el sistema de control de versiones administra el almacenamiento de programas fuente. Allí se registran datos del desarrollador, fecha, hora y tamaño de los fuentes y objetos o ejecutables, de ser pertinente,
- donde corresponda, el implementador lleva a cabo procedimientos de compilación del programa fuente, dentro del ambiente de producción, y en el momento de realizar el pasaje. Con ello, puede garantizarse una correspondencia biunívoca con el ejecutable en producción. Al finalizar esta operación, el programa fuente se elimina del ambiente productivo, quedando sólo el ejecutable,
- en el pasaje a producción intervienen, donde sea pertinente, los administradores de la infraestructura y de las bases de datos.

7.1.4.7 Ambientes informáticos adicionales

Según las necesidades, la complejidad y la interdependencia entre sistemas, así como la capacidad de la infraestructura tecnológica del MTEySS, se podrán implementar ambientes adicionales dentro del esquema básico indicado en *7.1.4.1 Infraestructura básica.*

7.1.4.8 Controles de los ambientes informáticos

Se definirán e implementarán los siguientes controles:

- los usuarios no podrán tener accesos compartidos sobre los distintos ambientes. Las interfaces de los sistemas identificarán claramente sobre qué instancia se está realizando la conexión,
- los Responsables de Informática y de Seguridad de la Información definirán propietarios de la información para cada ambiente de desarrollo, prueba y homologación establecido,
- se impedirá el acceso al ambiente productivo a programas compiladores, editores y otros utilitarios de sistemas. Si este acceso es indispensable para el funcionamiento de un aplicativo en producción, el Responsable de Informática debe registrarlo e informarlo a los Responsables Primarios y de Seguridad de la Información,
- el personal de desarrollo no tendrá acceso al ambiente productivo. En caso de extrema necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos,
- los sistemas deberán contemplar funcionalidades para efectuar correcciones de datos por parte de los usuarios, a fin de evitar ulteriores accesos por parte de desarrolladores y/o implementadores, en el ambiente de Producción. Dichas funcionalidades estarán definidas por el Responsable Primario, junto con los Responsables de Seguridad de la Información y de Informática, antes de empezar el desarrollo del mismo,

- el acceso directo a bases de datos y/o tablas de usuarios del ambiente operativo, estará inhibido a usuarios, desarrolladores e implementadores. Se deben diseñar y poner en marcha sistemas e interfaces, donde corresponda, para las gestiones y/o el procesamiento de la información. P. ej.: se dispondrá de un sistema de gestión de identidades a los efectos de la administración de cuentas de aplicativos,
- se establecerán los controles compensatorios indicados en *7.1.3 Control: Separación de Funciones* para el caso que no se logre una adecuada separación física entre los distintos entornos.

En la cláusula *10.4 Categoría: Seguridad de los Archivos del Sistema*, se detallan especificaciones en cuanto a los perfiles y la seguridad a implementar sobre los ambientes de procesamiento.

7.2 Categoría: Gestión de Provisión de Servicios

Objetivo

Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio, en línea con los acuerdos de entrega de servicios establecidos con los Responsables Primarios, organizaciones externas y/o contratistas, donde corresponda.

Los Responsables de Seguridad de la Información, de Informática, del Administración y del Área Legal, donde corresponda, verificarán:

- la definición y la implementación de los acuerdos,
- el cumplimiento con los estándares y la normativa,
- la gestión de cambios para asegurar que los servicios sean entregados según lo acordado.

7.2.1 Control: Provisión de servicio

Se verificará que los contratos implementados con organizaciones externas y/o contratistas, incluyan -además de las definiciones de servicio y aspectos de la gestión- los requisitos de seguridad de la información del MTEySS que correspondan.

En casos de acuerdos de tercerización, al traspasar datos y/o instalaciones debe garantizarse el mantenimiento de un nivel adecuado de seguridad, a lo largo del período de transición.

Los aspectos de seguridad, los controles y el nivel de servicio serán acordados entre las organizaciones externas y/o contratistas, por un lado, y los Responsables de Seguridad de la Información, Responsable de Informática, de Administración y el Responsable del Área Legal del MTEySS, por el otro, y según corresponda.

El contrato de servicio abarcará los siguientes aspectos (Ver *2.3 Gestión con Grupos o personas externas*):

- identificar aplicaciones sensibles o críticas que no deberán transferirse a instalaciones de organizaciones externas y/o contratistas ,
- obtener la autorización de los Responsables Primarios cuyos sistemas serán transferidos,
- identificar las implicancias para la continuidad de las actividades del MTEySS, donde corresponda,
- especificar las normas de seguridad que deben cumplirse,
- establecer procedimientos de monitoreo de las actividades, y métricas para determinar el grado de cumplimiento de las normas,
- establecer funciones y procedimientos de gestión y comunicación de incidentes relativos a la seguridad.

7.2.2 Control: Seguimiento y revisión de los servicios de las organizaciones externas y/o contratistas

El MTEySS mantendrá un adecuado control sobre todos los aspectos de seguridad, con respecto a aquella información de su propiedad que sea accedida, procesada o gestionada por organizaciones externas y/o contratistas.

El MTEySS controlará la información de su propiedad, aún cuando ésta se encuentre en instalaciones ajenas. Se deberá mantener la visibilidad de las actividades, considerando lo siguiente:

- realizar seguimiento, control y revisión de los servicios de las organizaciones externas y/o contratistas,
- establecer procedimientos de gestión de cambios, acordados con las organizaciones externas y/o contratistas,
- verificar el cumplimiento de las políticas de seguridad de la información del MTEySS,
- establecer procedimientos de identificación de vulnerabilidades, gestión de incidentes de seguridad de la información y de resolución de problemas.

7.2.3 Control: Gestión del cambio de los servicios de organizaciones externas y/o contratistas

Se definirán procedimientos de gestión de cambio, tomando como base las políticas de seguridad de la información del MTEySS y la criticidad de los sistemas involucrados en las actividades de las organizaciones externas y/o contratistas.

7.2.3.1 Gestión de Cambios en el MTEySS

El proceso de gestión de cambios en el MTEySS, para servicios a organizaciones externas, deberá tener en cuenta:

- implementación de mejoras a los servicios existentes,
- desarrollo de nuevas aplicaciones y sistemas,
- modificaciones o actualizaciones de las políticas y procedimientos del MTEySS,
- nuevos controles para aumentar la seguridad,
- mejora en los procedimientos de resolución de incidentes de seguridad de la información.

7.2.3.2 Gestión de cambios de los contratistas

El proceso de gestión de cambios para los servicios que los contratistas brinden al MTEySS debe contemplar lo siguiente:

- cambios y mejoras de las redes que interconectan sistemas y datos del Organismo,
- uso de nuevas tecnologías y/o productos de software,
- nuevas herramientas de desarrollo y ambientes, según corresponda,
- cambio de las ubicaciones físicas de las instalaciones de servicios al MTEySS.

7.2.4 Control: Servicios en la nube

Los servicios informáticos en la nube (*cloud computing*) son un ejemplo de las actividades de contratistas u organizaciones externas que involucran a la información del MTEySS.

7.2.4.1 Seguridad Física y Condiciones Ambientales

El Responsable de Seguridad de la Información, con la colaboración del Responsable de Seguridad Física y el Responsable de Informática, donde corresponda, establecerá los requerimientos de seguridad física y condiciones ambientales exigibles en las instalaciones informáticas del proveedor de servicios de nube.

Se tomará como base que la seguridad física ambiental ofrecida deberá tener niveles iguales o superiores a los existentes en las instalaciones de procesamiento del MTEySS.

Se dispondrá de mecanismos tales como: controles de temperatura y humedad, detectores de humo y sistemas de supresión de incendios.

7.2.4.2 Gobernabilidad de los servicios

La gobernabilidad permitirá la continuidad y la seguridad de los servicios implementados en la nube. El enfoque de control y de políticas de seguridad en los servicios de nube deberá ser más restrictivo que el empleado en la infraestructura del MTEySS.

Los siguientes factores garantizarán un adecuado control del MTEySS sobre los servicios:

- *gestión contractual entre el proveedor del servicio de nube y el MTEySS*, estableciendo un acuerdo que identifique los procesos de control y de auditoría,
- *gestión de riesgos*, que permita identificar la infraestructura, los servicios en la nube, las amenazas y los mecanismos para mitigarlas,
- gestión de cumplimiento de la normativa, para garantizar la protección de los datos, en función de aspectos jurisdiccionales, contractuales y de legislación nacional,
- *gestión de seguridad de la información*, estableciendo procedimientos de control de accesos y monitoreo, definiendo perfiles y separación de tareas, y aplicando compromisos de confidencialidad,
- *gestión de la disponibilidad*, estableciendo, en los acuerdos, los tiempos de respuesta ante incidentes, los planes de continuidad, restauración y/o migración de los servicios puestos en la nube,
- *gestión de interoperabilidad*, asegurando que exista una integración eficiente y eficaz entre los servicios de nube y la infraestructura del MTEySS.

7.3 Categoría: Planificación y Aprobación de Sistemas

Objetivo

Se requiere planificar la capacidad de los recursos informáticos, en forma anticipada, de forma de asegurar una disponibilidad que permita un desempeño eficiente de los sistemas.

Se realizarán proyecciones de los requerimientos futuros de la capacidad, a fin de reducir el riesgo de sobrecarga en el sistema.

Se deben establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos, antes de su aceptación y uso.

7.3.1 Control: Planificación de la Capacidad

El Responsable de Informática tendrá a su cargo el monitoreo de las necesidades de capacidad de los sistemas en operación y la proyecciones de demanda futura.

Para ello se tendrá en cuenta:

- la definición de nuevos requerimientos para los sistemas informáticos,
- las tendencias actuales y proyectadas en el procesamiento de la información del MTEySS, según el período de vida útil estipulado para cada componente,
- la identificación de potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento.

7.3.2 Control: Aprobación del Sistema

Tanto el Responsable de Informática como el Responsable de Seguridad de la Información determinarán criterios de aprobación para liberar a los usuarios los sistemas de información nuevos, así como las actualizaciones y nuevas versiones de aplicativos instalados.

Asimismo, los criterios serán acordados formalmente con los Responsables Primarios. En cada caso, se efectuarán todas las verificaciones y pruebas necesarias, antes que se otorgue la aprobación definitiva.

Se tendrán en cuenta los siguientes puntos:

- verificar el impacto en el desempeño y los requerimientos de capacidad del equipamiento informático y de comunicaciones empleados,
- garantizar la recuperación ante errores de operación y procesamiento,
- establecer y probar los procedimientos operativos de rutina, según normas definidas,
- garantizar la implementación de un conjunto adecuado de controles de seguridad,
- establecer procedimientos relativos a la continuidad de las actividades del MTEySS,
- garantizar que una nueva instalación no impacte negativamente sobre la performance de los sistemas existentes, especialmente en los períodos de procesamiento pico,
- verificar el impacto que un nuevo sistema tenga sobre la seguridad global del MTEySS,
- capacitar a los usuarios finales en la operación y/o uso de nuevos sistemas.

7.4 Categoría: Protección Contra Código Malicioso

Objetivo

Los sistemas y medios de procesamiento de la información son vulnerables a la introducción de código malicioso y/o código móvil no-autorizado, p. ej.: virus Troyanos, bombas lógicas, etc.

Para proteger la integridad de los sistemas informáticos y los datos del MTEySS, se requiere la implementación de procesos y mecanismos que permitan detectar y/o evitar la introducción de tanto código malicioso como código móvil no autorizado.

Se debe concientizar a los usuarios sobre las precauciones a tener en cuenta para mitigar o evitar que este tipo de programas maliciosos se filtren hacia los recursos de información del MTEySS.

7.4.1 Control: Código Malicioso

7.4.1.1 Responsabilidades

El Responsable de Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso, los que serán implementados por el Responsable de Informática.

Por otra parte, el Responsable de Seguridad de la Información, colaborando con el Responsable de Capacitación, desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

7.4.1.2 Controles

Se formalizarán procedimientos de control que contemplen las siguientes acciones:

- prohibir la instalación y uso de software no autorizado por el Organismo (ver *12.1.2 Control: Derecho de Propiedad Intelectual del Software*),
- redactar procedimientos para mitigar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio (ej.: dispositivos portátiles), señalando las medidas de protección a tomar,
- redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos,
- instalar y actualizar sistemas de detección y reparación de virus, estableciendo procesos centralizados y rutinarios para verificar de equipos y medios informáticos,

- instalar los últimos parches de seguridad disponibles para los sistemas operativos, manteniendo la periodicidad de actualización establecida por el proveedor. Implementar entornos de prueba para dichas actualizaciones, para prevenir el riesgo de un compromiso sobre los sistemas existentes,
- revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del MTEySS, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas,
- establecer criterios y procedimientos para validar los programas informáticos y datos existentes en los puestos de trabajo, equipos de procesamiento y dispositivos móviles, tanto de propiedad del MTEySS como de aquellos recursos personales que accedan a la red del Organismo,
- efectuar un análisis de logs de puestos de trabajo y equipos de procesamiento, donde corresponda,
- verificar, antes de su uso, la presencia de virus en archivos almacenados en medios electrónicos de origen incierto, o recibidos a través de redes no confiables,
- concientizar al personal sobre cómo proceder frente a la presencia de falsos antivirus (*rogues*), cadenas falsas (*hoax*) y técnicas de suplantación y/o robo de identidad (p.ej.: *phishing*),
- redactar normas de protección, habilitación de puertos de conexión y derechos de acceso a dispositivos móviles (pendrives, discos externos, teléfonos inteligentes, etc.).

7.4.2 Control: Código Móvil

Se debe garantizar que la configuración asegure que todo código móvil autorizado opere de acuerdo a una configuración de seguridad claramente definida. Por otra parte, la configuración deberá impedir la ejecución de todo código móvil no autorizado.

Asimismo, se implementarán las siguientes protecciones para evitar riesgos surgidos de la ejecución no autorizada de código móvil:

- ejecución del código móvil en un ambiente lógicamente aislado,
- bloqueo del uso y recepción de código móvil,
- activar las medidas técnicas que estén disponibles, para asegurar la administración del código móvil,
- control de los recursos disponibles para el acceso del código móvil,
- implementación de controles criptográficos para autenticar de forma unívoca el código móvil.

7.5 Categoría: Resguardo de la información del MTEySS

Objetivo

Mantener la integridad y la disponibilidad de la información y los medios de procesamiento del MTEySS.

Para cumplir con el objetivo, se debe establecer una política, a partir de la cual se desarrollarán procedimientos para el respaldo, la restauración y la guarda de los datos del MTEySS (ver también *Capítulo 11.1 Gestión de Continuidad del Organismo*).

7.5.1 Control: Resguardo de la Información

7.5.1.1 Responsabilidades

Los Responsables de Informática y de Seguridad de la Información, junto a cada Responsable Primario, determinarán las políticas de resguardo de los sistemas y los datos del MTEySS.

Dichas políticas deberán basarse en un análisis de riesgos y la criticidad de la información establecida.

El Responsable de Informática implementará los siguientes procesos:

- realización de copias de resguardo,
- restauración de información o sistemas, para resolver contingencias,
- verificación periódica de las copias de resguardo,
- guarda de la información crítica, en cualquier tipo de medio de almacenamiento.

7.5.1.2 Procedimientos

Las operaciones de resguardo y restauración deben respetar lo indicado en el *Capítulo 4 Gestión de Activos* y el capítulo *12.1.3 Control: Protección de los Registros del Organismo* de la presente Política.

Las políticas y los procedimientos deben considerar los siguientes factores:

- existencia de copias de respaldo de la información. Se efectuará copia de todos los sistemas y datos, para asegurar la continuidad de las operaciones del MTEySS,
- parámetros para los procesos de resguardo. Se partirá de un análisis de riesgos y del nivel de disponibilidad establecido en la clasificación (ver *Capítulo 4.2 Clasificación de la Información*). P. ej.: se definirán los tiempos de recuperación sin que se pierdan datos (RPO) y los plazos necesarios para comenzar la recuperación (RTO), requeridos para minimizar cualquier impacto negativo sobre la gestión del MTEySS,
- tipos de repositorios de resguardo. Considerando esquemas de resguardo completo, diferencial y/o incremental, se buscará el mejor aprovechamiento de la capacidad disponible en los medios de resguardo,
- gestión de los repositorios de información. Se deberá establecer un esquema de administración, considerando: resguardo en línea, resguardo fuera de línea y/o centros de resguardo,
- medios de resguardo. Se establecerá que medios de resguardo se utilizarán en función del tipo de gestión de los repositorios. P. ej.: discos o arreglos de disco (más adecuados para los resguardos en línea), cintas (más adecuados a los resguardos fuera de línea y a los centros de resguardo), discos ópticos (para un esquema de retención prolongado), etc.
- esquemas de rotación. Se establecerá un esquema adecuado de niveles de disponibilidad y reutilización de los medios de resguardo, p. ej.: esquema abuelo-padre-hijo.
- pautas de retención y conservación de datos. Se tendrán en cuenta los requisitos legales y/o normativos de los sistemas de manera de establecer los períodos de conservación de la información a resguardar,
- administración de los medios. Para una gestión eficiente, se definirá un esquema de rotulación de las copias de resguardo, de forma de contar con toda la información necesaria para identificar a cada una de ellas (Ver *Capítulo 4.3 Etiquetado y manipulado de la información*),
- pruebas de recupero de información. Se efectuarán verificaciones periódicas de recupero de información, en función de la criticidad de la información almacenada en ellos,
- controles de las operaciones de resguardo y recupero. Se dispondrá de procesos de monitoreo y/o auditoría para las operaciones de resguardo y recupero. Se deberán registrar, entre otros, datos como los tiempos insumidos para el resguardo, la verificación de quién y por qué solicita restauración de datos, la registración de operaciones interrumpidas y la verificación de integridad de los datos resguardados,
- remplazo de los medios de las copias de resguardo. Se establecerán procedimientos que verifiquen el tiempo de uso de los medios, y la posibilidad de ser reutilizados, según especificaciones del proveedor. Se definirán, además, los procedimientos de destrucción, cuando corresponda (Ver *Capítulo 4.7.2 Eliminación de Medios de Información*),

- protecciones de acceso físico y ambiental. Los dispositivos de resguardo y recupero deberán gozar de las mismas protecciones que los sitios de procesamiento de la información. Los medios de resguardo, por otra parte, deben almacenarse en ámbitos y recintos que cumplan con los requisitos indicados por el proveedor de dichos medios. P. ej.: se debe considerar la utilización de armarios con alta robustez y con características ignífugas,
- guarda externa de medios. Como parte de los esquemas de contingencia, se verificará la contratación de servicios de guarda externa de los medios que contengan información crítica del MTEySS. Se deberá verificar el establecimiento de los mismos controles de protección física y ambiental que se hallan aplicados en los sitios de resguardo del Organismo, tanto en lo referente a manipulación como a la custodia y el traslado de los medios entre las sedes del MTEySS y las del proveedor de la guarda. (Ver *Capítulo 4.8.3 Seguridad de los Medios en Tránsito*).

7.5.2 Control: Registro de Actividades del Personal Operativo

El Responsable de Informática implementará un registro de las actividades realizadas en los sistemas informáticos.

La Unidad de Auditoría Interna contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

Los registros incluirán la siguiente información, según corresponda:

- tiempos de inicio y cierre del sistema,
- errores del sistema y medidas correctivas tomadas,
- intentos fallidos de acceso a sistemas, recursos o información crítica,
- intentos de ejecución de acciones restringidas,
- ejecución de operaciones críticas,
- modificaciones sobre la información crítica.

7.5.3 Control: Registro de Fallas

El Responsable de Informática implementará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o en las comunicaciones, de manera que se permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, en el marco de un proceso de gestión de incidentes. Se deben considerar los siguientes aspectos:

- revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
- revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
- documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.
- integrar la comunicación y la gestión de la falla, según procesos definidos en el Capítulo 11 Gestión de Incidentes.

7.6 Categoría: Gestión de la Red

Objetivo

Asegurar la protección de la información que se transmite por las redes, tanto internas como externas al MTEySS.

La gestión segura de las redes abarca más allá de los límites organizacionales, requiriendo por lo tanto una cuidadosa consideración de los flujos de datos, las implicancias legales, un monitoreo

estricto y una protección integral. Se requiere, además, el análisis de la implementación de controles adicionales para proteger la información del MTEySS que pasa a través de redes públicas.

7.6.1 Control: Controles en las Redes

El Responsable de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo, contra el acceso no autorizado. Dichos controles serán implementados por el Responsable de Informática.

Se deberá considerar lo siguiente:

- la administración de la infraestructura de la red de datos estará separada de la administración y/u operación de los puestos de trabajo,
- la implementación de controles especiales para salvaguardar el procesamiento y la disponibilidad de los datos que pasan a través de redes públicas, p. ej.: a través de servicios de Redes Privadas Virtuales o en conexiones a la nube,
- la aplicación, donde corresponda, de tecnologías de protección, tales como encriptación, autenticación y controles de conexión a la red.

7.6.2 Control: Verificaciones de Seguridad en los Servicios de Red

Se deberá considerar la ejecución de las siguientes acciones:

- definir procedimientos para la administración de los puestos de trabajo en las áreas de usuarios del MTEySS, incluyendo a los equipos personales conectados a las redes del Organismo. Esta acción será coordinada con los Responsables Primarios, cuando corresponda (Ver *Capítulo 2.4 Utilización de Recursos Informáticos Personales*),
- definir procedimientos para la administración de dispositivos móviles propiedad del MTEySS, incluyendo los equipos personales conectados a las redes del Organismo. Esta acción será coordinada con los Responsables Primarios, cuando corresponda (Ver *Capítulo 2.4 Utilización de Recursos Informáticos Personales*),
- la identificación y registración adecuada de los dispositivos y equipamiento conectado a la red de datos del MTEySS,
- verificar que los controles se aplican uniformemente en toda la infraestructura y en todos los nodos de procesamiento y transmisión de la información.

7.7 Categoría: Administración y Seguridad de los medios de almacenamiento

Objetivo

Los medios se deben controlar y proteger físicamente, a fin de evitar la divulgación no-autorizada del MTEySS, así como la modificación, eliminación o destrucción de activos (Ver *Capítulo 4.1.2 Inventario de Activos*)

Se deben establecer procedimientos que garanticen una operación segura sobre:

- documentos en papel, medios informáticos de almacenamiento,
- entrada/salida de datos,
- documentación de sistemas informáticos (configuraciones de infraestructura, listados de programas),
- paquetes de software.

7.7.1 Control: Administración de Medios Informáticos Removibles

Los Responsables de Informática y de Seguridad de la Información, junto con el Responsable de Seguridad Física y los Responsables Primarios, cuando corresponda, definirán e implementarán

procedimientos para la administración de medios informáticos removibles, cumpliendo lo indicado en los Capítulos 9.1 *Categoría: Requerimientos para el Control de Acceso* y *4.1.2 Control: Inventario de activos*.

7.7.1.1 Medios Removibles

Sin ser exhaustiva, dada la creciente variedad de dispositivos removibles, se consideran a los siguientes:

- documentos impresos,
- cintas de impresión de un solo uso y papel carbónico,
- medios de almacenamiento magnético (cintas y cartuchos de cinta) y óptico (CD, DVD),
- memorias portátiles (*pendrives*, *SIMMs*), discos removibles, dispositivos móviles (teléfonos inteligentes, tabletas, *netbooks*, *notebooks*), dispositivos de almacenamiento de conexión USB, tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

7.7.1.2 Procedimientos de control de medios removibles

Los procedimientos deben considerar las siguientes acciones:

- eliminación segura del contenido, cuando ya no se requiere, o antes de reutilizar el medio,
- autorización, por parte del Responsable Primario, para retirar cualquier medio del Organismo,
- control de entrada o salida de los medios removibles, manteniendo un registro de auditoría,
- almacenamiento de los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones del fabricante y de la criticidad de la información almacenada.

7.7.2 Control: Eliminación de Medios de Información

Los Responsables de Informática y de Seguridad de la Información, junto con el Responsable de Seguridad Física y los Responsables Primarios, cuando corresponda, implementarán procedimientos para la eliminación de medios de información.

Se deberá implementar una evaluación de riesgos y considerar el nivel de criticidad de la información contenida, para determinar el mecanismo de eliminación más adecuado.

7.7.3 Control: Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información, según lo establecido en los Capítulos 4.1.2 Control: Inventario de activos y *4.2 Categoría: Clasificación de la información*.

7.7.3.1 Elementos a proteger

Se deberá proteger la información contenida, transmitida o almacenada en:

- documentos en papel,
- sistemas informáticos,
- redes internas y conexiones a redes externas, p. ej.: accesos a servicios de procesamiento en la nube,
- puestos de trabajo del MTEySS, dispositivos personales,
- computación móvil y comunicaciones móviles,
- servicios de correo postal, correo de voz, comunicaciones de voz en general, servicios multimedia,
- servicios e instalaciones postales,