- máquinas de fax.

7.7.3.2 Definiciones a considerar

En los procedimientos se contemplará lo siguiente:

- sólo permitir accesos al personal debidamente autorizado,
- mantener un registro formal de las personas autorizadas a recibir o enviar datos,
- garantizar que los datos de entrada están completos y corresponden con las definiciones establecidas,
- garantizar que el procesamiento se lleva a cabo correctamente, y que las salidas son validadas,
- proteger los datos en espera (colas) y en memorias temporales (p. ej.: en cache),

7.7.4 Control: Seguridad de la Documentación del Sistema

La información documentada de los sistemas informáticos debe tratarse como de uso restringido o confidencial. Los accesos serán autorizados por cada Responsable Primario a cargo de la información que corresponda, implementados por el Responsable de Informática, y verificados po el Responsable de Seguridad de la Información, según corresponda.

Se deben considerar los siguientes recaudos para su protección:

- almacenar la documentación de los sistemas en forma segura,
- autorizar el acceso a la documentación de los sistemas al personal estrictamente necesario.

7.8 Categoría: Intercambio de Información y Software

Objetivo

El intercambio de información y software, dentro del MTEySS y con cualquier otra entidad externa, debe efectuarse en condiciones seguras.

El intercambio de información y/o software debe basarse en acuerdos formales de intercambio, en línea con las políticas de seguridad establecidas, y con la legislación pertinente ver *Capítulo 12 Cumplimiento*).

Se deben establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en tránsito.

7.8.1 Control: Procedimientos y controles de intercambio de la información

Se establecerán procedimientos y controles formales para proteger el intercambio de datos, a través de los distintos medios de comunicación (Ver *Capítulo 2.1.4 Control: Compromisos de confidencialidad* y *6.2.3 Control: Riesgos relacionados con grupos externos*)

Se deberá considerar lo siguiente:

- proteger a la información contra intercepción, copiado o modificación no autorizados, dirección de envío o recepción erróneas, y destrucción no planificada,
- detección y protección contra código malicioso introducido durante el uso de comunicaciones electrónicas,
- definición de requisitos de uso aceptable de las comunicaciones electrónicas,
- definición de pautas de uso seguro de las comunicaciones inalámbricas,
- responsabilidades de uso, por parte del personal, organizaciones externas y/o contratistas que accedan a la información y/o recursos del MTEySS, p. ej:
  - no utilizar las instalaciones del Organismo para hostigar y/o difamar,
  - no producir bloqueos o interferencia sobre los accesos físicos o lógicos,

- no efectuar suplantación o robo de identidad,
- no efectuar envío de cadenas de mensajes de correo sin autorización,
- no efectuar compras por medios electrónicos, cuando éstas no estén autorizadas por un Responsable Primario,
- no efectuar comunicaciones a redes sociales cuando éstas tengan fines personales o no autorizados,

- concientización al personal, organizaciones externas y/o contratistas, cuando corresponda, sobre las precauciones que deben tomar a la hora de transmitir información del MTEySS,
- uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información, cuando corresponda.

7.8.2 Control: Acuerdos de Intercambio de Información y Software

Los acuerdos para intercambio de datos entre el MTEySS y otras organizaciones deben especificar el grado de sensibilidad y las consideraciones de seguridad sobre información involucrada.

Se tendrán en cuenta los siguientes aspectos:

- procedimientos y responsabilidades en las gestiones de control y notificación de transmisiones, envíos y recepciones,
- normas y controles técnicos para la transmisión, la confidencialidad, la integridad y la autenticidad de la información transmitida, p. ej.: empleo de criptografía y/o firma digital,
- pautas para la identificación y la validación del prestador de comunicaciones,
- responsabilidades y obligaciones, en caso de pérdida, exposición o divulgación no autorizada de datos,
- procesos de resguardo y recupero de la información transmitida,
- acuerdo sobre el empleo de un sistema común, para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida,
- términos y condiciones de licencia, cuando se suministra software,
- requisitos uso y propiedad de la información que se suministra,
- normas técnicas para la grabación y lectura de la información y del software.

7.8.3 Control: Seguridad de los Medios en Tránsito

Los procedimientos de transporte, mediante envío postal o servicios de mensajería, de medios informáticos entre diferentes puntos deben contemplar:

- *verificación de confiabilidad de los medios de envío postal o servicios de mensajería.* El Responsable Primario determinará el servicio a utilizar, tomando como base la criticidad de la información a transmitir,
- *embalaje adecuado para envíos a través de servicios postales o de mensajería.* Se seguirán las especificaciones de los fabricantes o proveedores,
- *controles especiales, cuando resulte necesario.* Entre los ejemplos se incluyen:
  - uso de envoltorios y/o recipientes adecuados al tipo de información que se transforma (p. ej.: cajas especiales para el transporte de medios que se envían a guarda externa),
  - entrega en mano, con verificación del remitente y constancia de recepción,
  - embalaje a prueba de apertura no autorizada, garantizando que pueda detectarse cualquier intento de acceso fallido,

- en casos excepcionales, fraccionar los envíos en más de una entrega, empleando diferentes rutas.

7.8.4 Control: Seguridad de la Mensajería

La mensajería electrónica, tal como el correo electrónico (e-mail, del inglés), el intercambio de datos electrónicos (*EDI*, por sus siglas en inglés), la mensajería instantánea (*chat*, del inglés) y las redes sociales, juegan un muy importante rol en las comunicaciones de toda organización.

A diferencia de los mensajes en papel, los riesgos en las comunicaciones basadas en mensajería electrónica tienen carácter crítico para el MTEySS. Para el caso del correo electrónico aplicado en el MTEySS, ver el *Capítulo 7.9 Categoría: Seguridad del Correo Electrónico*.

Se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

- protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio,
- controles de autenticación fuerte, de manera de verificar adecuadamente tanto el destino del mensaje, como el remitente,
- confiabilidad y disponibilidad general del servicio,
- control de uso, prohibiendo la utilización con fines personales,
- consideraciones legales, por ejemplo, requerimientos para firmas electrónicas,
- obtención de aprobación previa para el uso de servicios externos al MTEySS, p. ej.: mensajería instantánea, redes sociales o correo de internet privado (p. ej.: dominios de correo como *Yahoo, Google, Hotmail*, entre otros), servicios de archivos compartidos (p. ej.: *Bitorrent, Mega*, entre otros) y transmisión multimedia (p. ej.: *Netflix*, entre otros),

7.8.5 Control: Seguridad del Gobierno Electrónico

El Gobierno Electrónico constituye un medio de intercambio de datos esencial para la gestión del MTEySS. Entre ellos, se destacan los trámites en línea (p. ej.: presentaciones ante el Estado y entre las organizaciones) y los procesos de oferta y contratación pública.

El Responsable de Seguridad de la Información, junto con los Responsables Primarios, verificará los procedimientos de aprobación y uso, para las aplicaciones de Gobierno Electrónico, siguiendo lo establecido en los puntos *7.3.2 Control: Aprobación del Sistema* y *12.3.1 Control: Política de Utilización de Controles Criptográficos*.

Los procesos y los controles serán implementados por el Responsable de Informática.

Los Responsables Primarios de los procesos vinculados a Gobierno Electrónico difundirán entre los usuarios los términos y condiciones de uso establecidos.

Por otra parte, las medidas vinculadas al Plan de Gobierno Electrónico del MTEySS se dictarán conforme la normativa vigente, destacándose lo dispuesto por el *Decreto Nº 378/2005*.

7.8.5.1 Controles y procesos para el Gobierno Electrónico

Las aplicaciones de Gobierno Electrónico deben incluir los siguientes aspectos:

- *autenticación*. Se establecerá un nivel de confianza recíproca suficiente sobre la identidad del usuario y el MTEySS,
- *autorización*. Los Responsables Primarios deberán definir niveles de autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Los mismos serán comunicados al receptor de la transacción electrónica,
- *no repudio*. Se emplearán técnicas de firma digital, a los fines de evitar que se pueda negar acciones como el envío o la recepción de datos,

- *integridad*. Se deberá minimizar el riesgo que la información y las aplicaciones se alteren en su contenido, se infecten con código malicioso o sean vulnerables debido a deficientes prácticas de desarrollo,
- *confidencialidad*. Se utilizarán técnicas criptográficas, a fines de codificar la información sensible que se transmita,
- *protección a la duplicación*. Los controles de transmisión deberán asegurar que una transacción sólo se realizará una vez, a menos que se especifique lo contrario,
- *cierre de la transacción*. Los procesos de transmisión establecerán la interacción de cierre más adecuada, a los fines de evitar fraudes,
- *responsabilidades operativas*. Se establecerán las responsabilidades que correspondan, para evitar riesgos de presentaciones, tramitaciones o transacciones fraudulentas,

7.9 Categoría: Seguridad del Correo Electrónico

Objetivo

Garantizar la protección de los datos, considerando, asimismo, las implicancias de seguridad asociadas con los servicios de correo electrónico del MTEySS, también denominado genéricamente como correo corporativo.

7.9.1 Control: Riesgos de Seguridad

Se implementarán controles para mitigar riesgos de seguridad en el servicio del correo corporativo, tales como:

- vulnerabilidades de los mensajes por acceso no autorizado o por violación de la integridad,
- manejo inadecuado o malicioso de los mensajes, produciendo denegación de servicios,
- intercepción y acceso no autorizado a los mensajes y/o a los servicios de distribución de correo,
- recepción de código malicioso en un mensaje de correo, produciendo un impacto en la seguridad del servicio, de la terminal receptora o de la red de datos del MTEySS,
- falta y/o deficiencia en los controles de prueba de origen, envío, entrega y aceptación,
- incumplimiento de consideraciones legales y uso inadecuado por parte del personal,
- implicancias en la confiabilidad y la disponibilidad general del servicio,
- el impacto de cambios en la plataforma de comunicaciones del MTEySS,
- acceso remoto (p. ej.: vía plataforma Web) a la plataforma de correo corporativo del MTEySS,
- implicancias de la publicación no autorizada de información sensible o confidencial.

7.9.2 Control: Política de Correo Electrónico

El Responsable de Seguridad de la Información definirá y documentará normas y procedimientos claros con respecto al uso del correo corporativo. Los controles serán implementados por el Responsable de Informática.

7.9.2.1 Aspectos del Uso del Correo Corporativo

Se definirán los siguientes aspectos:

- alcances del uso del correo electrónico por parte de los usuarios,
- controles para el buen funcionamiento del servicio, tales como:
  - tamaño máximo del mensaje transmitido y/o recibido,
  - cantidad de destinatarios,

- tamaño máximo del buzón del usuario,
- tipos de archivos autorizados como adjuntos en los mensajes,

- protecciones contra software malicioso y acceso no autorizado, tales como: antivirus para los mensajes y archivos adjuntos, y control de correo no deseado,
- interconexión del servicio de correo con aplicativos y sistemas que así lo requieran,
- definición de tipos de cuentas y responsabilidades de uso, p. ej.: cuentas de usuario, grupales y/o genéricas, etc.,
- empleo de técnicas criptográficas y firma digital, para asegurar la confidencialidad, la integridad y la autenticidad de los mensajes (Ver 9.3 Categoría: Controles Criptográficos),
- resguardo, recuperación y período de retención de los archivos de correo,
- utilización de mensajes de correo para casos de litigio.

7.9.2.2 Empleo del Correo Corporativo por parte de los usuarios

El correo electrónico es uno de los recursos, propiedad del MTEySS, que se proporciona al personal y a usuarios externos autorizados, con el fin de apoyar la gestión cotidiana del Organismo.

En virtud de la normativa vigente, y a la par de proteger sus recursos, el MTEySS deberá salvaguardar el derecho a la intimidad y la dignidad de las personas.

Por tales motivos, los usuarios de la plataforma informática del correo corporativo del MTEySS deberán estar claramente informados de lo siguiente:

- el MTEySS tendrá plena potestad para auditar los mensajes recibidos o emitidos por los servidores de correo. Esta política estará incluida en los Compromisos de Confidencialidad y/o Notificaciones de Uso Adecuado de los recursos, según corresponda,
- el Responsable de Seguridad de la Información establecerá las condiciones bajo las que se efectuarán tareas de control y monitoreo de los mensajes. Se solicitará la participación del Área Legal y/o de la Unidad de Auditoría Interna, en la implementación de los procedimientos, cuando corresponda,
- el Responsable de Seguridad de la Información y el Responsable de Recursos Humanos, cuando corresponda, indicará cuál es el uso que espera que su personal haga del correo corporativo,
- el Responsable de Informática implementará los controles de protección de la información y de la plataforma de correo electrónico del MTEySS, en función de lo definido por el Responsable de Seguridad de la Información,
- se prohibirá el uso del correo corporativo para fines particulares, así como se evitarán los abusos, el derroche o el desaprovechamiento. P. ej.: sólo se permitirá a personas autorizadas el envío de mensajes grupales o masivos,

7.9.2.3 Correo Electrónico Personal

Toda casilla de correo electrónico personal (p.ej.: casillas de coreo de Yahoo, Google y Hotmail, entre otras), instalada en un puesto de trabajo del MTEySS, configura situaciones de riesgo por la posibilidad de violar la confidencialidad de los datos personales y del propio Organismo.

El MTEySS no ejercerá potestad ni responsabilidad alguna sobre el correo electrónico personal que se halle instalado en puestos de trabajo de la Organización.

El Responsable de Informática podrá desinstalar esta clase de sistemas en los puestos de trabajo.

7.9.3 Control: Seguridad de los Sistemas Electrónicos de Oficina

El Responsable de Seguridad de la Información definirá lineamientos para controlar riesgos de seguridad relacionados con los sistemas de oficina, con la participación de los Responsables Primarios, siendo éstos implementados por el Responsable de Informática.

Dentro de los sistemas de oficina se incluyen los siguientes elementos:

- *puestos de trabajo*,
- computadoras personales y dispositivos de almacenamiento móvil, propiedad del MTEySS o de usuarios autorizados,
- sistemas móviles de computación, autorizados para ser utilizados dentro de la infraestructura informática del MTEySS,
- dispositivos de comunicación de voz (telefonía en sus diversas manera) o en papel (fax),
- sistemas multimedia,

7.9.3.1 Pautas para los sistemas de oficina

Se considerarán las implicancias para la seguridad y las actividades del MTEySS, incluyendo:

- procedimientos y controles para administrar la adecuada distribución y organización de la información,
- identificación de roles y funciones del personal, organizaciones externas y/o contratistas a quienes se les proporciona acceso a sistemas,
- controles de acceso a las instalaciones,
- requerimientos de soporte técnico y reposición de partes en garantía,
- acceso remoto a los servicios informáticos (por. ej.: redes privadas virtuales, sistema de correo web, etc.),
- configuración de controles de seguridad en los puestos de trabajo,
- políticas de seguridad para telefonía,
- control de almacenamiento de información laboral en servidores, exclusivamente, garantizando un adecuado recupero, cuando se lo requiera,
- control de la administración del puesto de trabajo (p. ej.: restringir posibilidades que el usuario instale o no programas, elimine archivos, etc.),
- controles sobre vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas y/o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.
- límites a la información brindada sobre las actividades que desarrollan determinadas personas, p. ej.: Autoridades del MTEySS, o personal que trabaja en proyectos sensibles.
- Compatibilidad, tanto del equipamiento informático como de las aplicaciones del MTEySS,
- perfiles del personal, organizaciones externas y/o contratistas, donde corresponda, autorizados a los usos de los sistemas de oficina, así como las ubicaciones físicas del equipamiento,
- restricciones de acceso físico y/o lógico a determinadas instalaciones, cuando corresponda,
- identificación de los usuarios, así como sus perfiles de acceso y las ubicaciones y equipos a los que se autoriza su uso,
- establecer el uso y/o proceso de la información en los sistemas de oficina, obligando a que se acceda y almacenen los datos en los servidores informáticos del MTEySS,

- políticas de resguardo y retención, establecidas según y resguardo de la información almacenada en el sistema (ver *Capítulo 7.5 Resguardo de la Información del MTEySS*).

7.9.3.2 Sistemas de Archivos Compartidos

Se implementarán controles sobre los riesgos de seguridad relacionados con la información que se almacena y comparte en servidores.

Los controles serán definidos por el Responsable de Seguridad de la Información, junto con los Responsables Primarios, y serán implementados por el Responsable de Informática.

Se considerarán aspectos como:

- control de archivos no autorizados o personales,
- clasificación de la información almacenada,
- cuotas de almacenamiento permitido en recursos de archivos,
- resguardo y restauración de archivos,
- retención y definición de permisos de acceso,
- filtros de para permitir el almacenamiento de distintos tipos de archivos.

7.9.4 Control: Sistemas de Acceso Público

La información del MTEySS puesta a disposición al público en general debe ser protegida adecuadamente, para evitar que una modificación no autorizada provoque un impacto negativo sobre la reputación del Organismo.

Todo sistema del MTEySS que tenga acceso público, p. ej., a través de servicios de comunicación con Internet, debe cumplir con estrictas políticas de seguridad.

El Responsable de Informática, en conjunto con los Responsables Primarios, establecerá un proceso de autorización de uso, con organizaciones y/o personas antes que la información se ponga a disposición del público.

El Responsable de Informática implementará los accesos y los controles establecidos, con la verificación de cumplimiento por parte del Responsable de Seguridad de la información.

7.9.4.1 Controles generales para los sistemas de acceso público

Todos los sistemas informáticos del MTEySS con acceso público deben tener en cuenta lo siguiente:

- la información se obtendrá, procesará y difundirá de acuerdo con la legislación y la normativa vigente, en especial, la Ley de Protección de Datos Personales,
- la información ingresada al sistema de publicación se procesará en forma completa, exacta y oportuna,
- se establecerán procedimientos para que la información sensible o confidencial sea protegida durante su recolección y almacenamiento,
- se establecerán controles que impidan accesos no autorizados o accidentales, tanto dentro del sistema de publicación como en las redes a las cuales éste se conecta,
- el encargado de la publicación de información en sistemas de acceso público se hallará claramente identificado y autorizado por el Responsable Primario que corresponda,
- el Responsable Primario que corresponda deberá garantizar la validez y la vigencia de la información publicada.

7.9.5 Control: Otras Formas de Intercambio de Información

Se implementarán normas, procedimientos y controles para proteger todo intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

Los Responsables Primarios, junto con los Responsables de Seguridad Física, de Seguridad de la Información, de Informática y de Recursos Humanos, cuando corresponda, establecerán, implementarán y concientizarán verificarán el cumplimiento de los siguientes controles :

- *llamadas telefónicas.* Se informará al personal sobre las precauciones que a tener en cuenta para no ser escuchado o interceptado, en los siguientes casos:
  - en presencia de personas cercanas, en especial al utilizar teléfonos móviles o inteligentes (*smartphones*),
  - a través de personas ajenas que tengan acceso a la comunicación, interviniendo la línea telefónica, entre varias formas de escucha subrepticias,
  - a través del acceso físico al aparato o línea telefónica, o mediante equipos de barrido de frecuencias al utilizar teléfonos móviles analógicos,
  - en presencia de terceros o ajenos en el lado receptor.
- *conversaciones de índole confidencial sobre datos del MTEySS.* El personal y/o terceros deberán cuidarse de hacer referencia a datos, procesos toda información de índole sensible en lugares públicos, oficinas abiertas y/o lugares de reunión con paredes delgadas.
- *mensajes en contestadores automáticos.* Ser cuidadoso al dejar mensajes en contestadores automáticos en sistemas públicos, ya que pueden almacenarse incorrectamente como resultado de un error de discado,
- *máquinas de fax.* Mitigar riesgos ocasionados por el uso de máquinas de fax, en particular:
  - acceso no autorizado a sistemas incorporados de almacenamiento de mensajes,
  - programación deliberada o accidental de equipos para enviar mensajes a números no verificados o sin autorizar,
  - envío de documentos y mensajes a un número equivocado por errores de discado o porque el número almacenado era erróneo.

7.10 Categoría: Seguimiento y control

Objetivo

A fin de detectar actividades de procesamiento de información no autorizadas, se deberá monitorear el uso de los sistemas de información del MTEySS, reportando todo evento que impacte sobre la seguridad de la información, y verificando el cumplimiento de la normativa legal relativa al monitoreo la auditoría.

Se dispondrá de registros de operación, identificando las fallas en los sistemas de información y la efectividad de los controles adoptados.

7.10.1 Control: Registro de auditoría

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, a los fines de permitir la detección e investigación de incidentes.

Se registrará la siguiente información:

- identificación de los usuarios,
- fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión,
- identidad del equipo y su ubicación, si es posible,
- registros de intentos de acceso al sistema exitosos y fallidos,
- registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados,
- cambios a la configuración del sistema,

- uso de privilegios,
- uso de utilitarios y aplicaciones de sistemas,
- archivos accedidos y el tipo de acceso,
- direcciones de redes y protocolos,
- alarmas que son ejecutadas por el sistema de control de accesos,
- activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.

7.10.2 Control: Protección de los registros

Se implementarán controles para la protección de los registros de auditoría contra cambios no autorizados y problemas operacionales, incluyendo:

- alteraciones de los tipos de mensajes que son grabados,
- edición o eliminación de archivos de registro,
- exceso de la capacidad de almacenamiento de los archivos de registro, con el riesgo que se produzcan fallas cuando se registran eventos, o se sobrescriban eventos registrados en el pasado.

7.10.3 Control: Actividades de los administradores

Se registrarán y revisarán periódicamente las actividades de los administradores de los sistemas, incluyendo:

- cuentas de administración u operación involucrada,
- momento en el cual ocurre un evento (éxito o falla),
- información acerca del evento (p. ej.: archivos manipulados) o de fallas (p. ej.: errores ocurridos y acciones correctivas tomadas),
- procesos involucrados.

7.10.4 Control: Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, debe verificarse la correcta configuración de los relojes de los equipos que procesan información del MTEySS.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, con una verificación con un patrón existente en una fuente externa del dato, considerándose además la modalidad de corrección ante cualquier variación significativa.

7.10.5 Control: Fallas reportadas por los usuarios

Se registrarán los fallos, efectuándose una revisión periódica de tales reportes, con el objetivo de tomar acciones apropiadas, considerando los requerimientos establecidos en el punto *7.5.3 Control: Registro de Fallas.*

8. Cláusula: Gestión de Accesos

Generalidades

La base de todo marco de gestión de seguridad de la información la proporciona un sistema de restricciones y excepciones para acceder a la información del MTEySS.

A través de la implementación de procedimientos formales, claramente documentados, difundidos y verificados, se garantizará el acceso adecuado y seguro a los sistemas, datos y demás servicios de información del MTEySS.

Los procedimientos comprenden todas las etapas del ciclo de vida del acceso a todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos para quienes ya no requieren usar los recursos del MTEySS.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario un proceso de concientización acerca de las responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

Esta cláusula tiene los siguientes objetivos:

- impedir el acceso no autorizado a los sistemas, datos y servicios de información,
- implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización,
- controlar la seguridad en la conexión entre la red informática del MTEySS y otras redes públicas o privadas,
- registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos informáticos,
- garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

Esta política se aplica a todas las formas de acceso sobre sistemas computacionales, conocidas también como *accesos lógicos*.

Están alcanzados todos los usuarios a quienes se les haya otorgado permisos sobre sistemas y aplicaciones, bases de datos, recursos y servicios informáticos del MTEySS, cualquiera sea la función o tarea que se desempeñe.

Se incluye, asimismo, al personal técnico que define, instala, administra, mantiene permisos de acceso y conexiones de red, y administran la seguridad informática.

Responsabilidad

El Responsable de Seguridad de la Información estará a cargo de:

- definir normas y procedimientos para:
  - la gestión de accesos a todos los sistemas, datos y servicios informáticos del MTEySS,
  - el monitoreo del uso de las instalaciones de procesamiento de la información, incluidos los recursos en la nube y la computación móvil,
  - los reportes de incidentes y la respuesta a la activación de alarmas silenciosas,
  - la revisión de registros de actividades y el ajuste de relojes de acuerdo a un estándar preestablecido.

El Responsable de Informática tendrá las siguientes responsabilidades:

- implementar procedimientos para la activación y desactivación de derechos de acceso a las redes,
- analizar e implementar los métodos de autenticación y control de acceso definidos, sobre los sistemas, bases de datos y recursos informáticos del MTEySS,
- evaluar, recomendar e implementar la plataforma de comunicaciones adecuada para subdividir la red de datos del MTEySS,
- implementar el control de uso de puertos de conexión y de ruteo de red,
- implementar y depurar el registro de eventos o actividades (logs) de usuarios, según lo definido por el Responsable de Seguridad de la Información y los Responsables Primarios, con la participación de la Unidad de Auditoría Interna,
- definir, implementar y controlar los registros de eventos y actividades correspondientes los sistemas operativos y demás plataformas de procesamiento de la información,
- evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de establecer tecnologías de identificación y autenticación de usuarios (p. ej.: biometría, verificación de firma y autenticadores de hardware), junto con el Responsable de Seguridad de la Información,
- definir e implementar las configuraciones de los servicios de red, de manera de garantizar una operación segura,
- analizar e implementar las medidas y controles para efectivizar el acceso a Internet de los usuarios,
- otorgar acceso a los servicios y recursos de red, verificando el cumplimiento de los procedimientos de autorización formales, a tal efecto.

Los Responsables Primarios estarán encargados de:

- definir los recursos de información que se requerirán para la gestión del área a su cargo, junto con el Responsable de Informática y de Seguridad de la Información,
- aprobar y solicitar formalmente la asignación accesos y privilegios de empleo de los recursos de información del MTEySS, de acuerdo las funciones que tenga el personal a su cargo,
- verificar que, en los procesos de desvinculación, se cumplan con los procedimientos de seguridad correspondientes, con los Responsables de Recursos Humanos, de Informática y de Seguridad de la Información, donde corresponda,
- solicitar el acceso a teletrabajo para el personal a su cargo,
- verificar que el personal a su cargo cumpla con las medidas de seguridad de la información.

El Responsable de Recursos Humanos será responsable de:

- notificar a los usuarios sobre los derechos y responsabilidades emanadas de los permisos de acceso a la información,
- determinar las pautas básicas de registro de las personas en los sistemas de información,
- verificar la especificación de sanciones ante la violación de los controles de acceso,

La Unidad de Auditoría Interna tendrá acceso a los registros de eventos a fin de colaborar con los controles, además de efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado, así como el período definido para el mantenimiento de los registros de auditoría generados.

Política

8.1 Categoría: Requerimientos para el Control de Acceso

Objetivo

Controlar el acceso a la información del MTEySS, sus medios de procesamiento de la información y los procesos de gestión, sobre la base de la seguridad.

Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información. Se establecerá la premisa de acceso prohibitivo (*Todo debe estar prohibido a menos que se permita expresamente*), por sobre la premisa permisiva (*Todo está permitido a menos que se prohíba expresamente*).

8.1.1 Control: Política de Control de Accesos

Se contemplarán los siguientes aspectos:

- identificación de los requerimientos de seguridad de cada una de los sistemas y aplicaciones informáticas del MTEySS,
- identificación de toda la información relacionada con los sistemas y las aplicaciones,
- definición de pautas que relacionen la política de control de accesos con la clasificación de la Información de los diferentes sistemas, aplicaciones y recursos informáticos (ver *capítulo 7 Gestión de Activos*),
- verificación de cumplimiento de las obligaciones contractuales de contratistas, con respecto a la protección del acceso a datos y servicios,
- establecimiento de perfiles de acceso relacionados con las definiciones de función y puesto laboral,
- administración de derechos de acceso acorde a la plataforma tecnológica del MTEySS.

8.1.2 Control: Reglas de Control de Acceso

Las reglas de control de acceso especificadas deben:

- ser de cumplimiento obligatorio,
- garantizar el control sobre las reglas de autorización de acceso, antes que éstas entren en vigencia,
- verificar que se controlen tanto los cambios automáticos en los permisos de usuario, iniciados por el sistema, como los manuales, iniciados por el administrador,
- verificar que se controlen tanto los cambios automáticos en los rótulos de información, iniciados por herramientas de procesamiento de información, como los manuales iniciados a discreción del usuario (Ver *capítulo 4 Cláusula: Gestión de Activos*).

8.2 Categoría: Administración de Accesos de Usuarios

Objetivo

Se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios informáticos, con el objetivo de impedir el acceso no autorizado a la información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, a saber:

- etapa inicial, otorgamiento de derechos de acceso a nuevos usuarios,

- etapa intermedia, cambio de derechos de acceso por nuevos requerimientos de trabajo, desplazamiento a otras áreas del MTEySS, o porque ya no se requieren.
- eliminación de los derechos por baja o inhabilitación de los usuarios.

8.2.1 Control: Registración de Usuarios

El Responsable de Seguridad de la Información definirá los procedimientos de registro de usuarios, siendo éstos implementados por el Responsable de Informática.

8.2.1.1 Pautas de control sobre la registración

Se contemplará lo siguiente:

- identificación unívoca de rótulos de información (ID de Usuario, perfiles y/o permisos de acceso, etc.), evitando la existencia de múltiples perfiles para un mismo usuario, y permitiendo un adecuado seguimiento (trazabilidad) de las operaciones efectuadas,
- control de modificaciones en los permisos de usuario, tanto de cambios automáticos como manuales,
- asignación de responsabilidades individuales sobre las tareas de autorización, administración, y operaciones,
- uso de cuentas personales individuales, a fin de poder efectuar un adecuado seguimiento de acciones y actividades por parte de los usuarios,
- cambios sobre los rótulos de información por medio de aplicativos o sistemas, inhibiéndose modificaciones manuales por parte del usuario,
- monitoreo y auditoría sobre accesos a recursos, sistemas y aplicativos,
- verificación de las autorizaciones formales por parte del Responsable Primario que corresponda,
- verificación sobre el nivel de acceso otorgado, de tal forma que sea adecuado a la función del usuario y que sea coherente con la política de segregación de tareas,
- listado detallado de los derechos de acceso de cada usuario, difundido a los Responsables Primarios,
- verificación de la firma de los Compromisos de Confidencialidad y Notificación de Uso Adecuado de los recursos, por parte de los usuarios,
- verificación sobre los procedimientos de implementación de accesos, asegurando que primero se hayan completado las autorizaciones correspondientes,
- verificación sobre la existencia de la aprobación y la justificación para implementar las excepciones,
- implementar, junto con el Responsable de Recursos Humanos cuando corresponda, las cancelaciones de acceso en tiempo y forma, evitando posibles daños o compromiso sobre la información del MTEySS,
- establecer pautas y procedimientos para la inhabilitación y/o eliminación de cuentas inactivas, los que serán implementados en colaboración con los Responsables Primarios y de Recursos Humanos, cuando corresponda.

8.2.1.2 Pautas de implementación

Deberán tenerse en cuenta los siguientes aspectos:

- identificación, autenticación de usuarios y administración de contraseñas,
- administración de permisos y perfiles,
- identificación y autenticación de nodos de red,

- uso controlado y restringido de utilitarios del sistema operativo, con el establecimiento de alarmas adecuadas,
- desconexión de terminales por tiempo muerto de uso, limitación del horario de conexión a la red, registro de eventos, limitación de puertos de acceso y control de conexiones,
- acceso lógico las instalaciones de procesamiento de información,
- tecnologías de identificación, autenticación de usuarios, integridad y no repudio, adecuadas para la Organización (Ej.: biometría, firma digital, etc.),
- sistemas centralizados para la administración de identidades, perfiles y accesos a los recursos del MTEySS,
- pautas de uso de Internet e Intranet,
- subdivisiones de la red (p. ej. mediante Redes LAN Virtuales),
- revisión periódica de permisos de acceso a la información,
- registros de auditoría sobre eventos,
- gestión de riesgos.

8.2.2 Control: Gestión de Privilegios

El acceso no autorizado a los recursos suele ser el factor de riesgo más importante para la seguridad de la información del MTEySS. Se requiere, por ende, una asignación de privilegios controlada.

Los Responsables Primarios aprobarán la asignación de privilegios de acceso a los recursos a su cargo. La implementación estará a cargo del Responsable de Informática, y la verificación de cumplimiento adecuado estará a cargo del Responsable de Seguridad de la Información.

8.2.2.1 Pautas para la gestión de los privilegios

Se deberá verificar lo siguiente:

- identificación de los privilegios asociados a cada recurso, sistema informático y/o aplicativo, p. ej.: la administración de los sistemas operativos, bases de datos y demás recursos informáticos, y/o el uso de las aplicaciones,
- establecimiento de distintas categorías de cuentas de acceso a los recursos, según la función, p. ej.: cuentas de usuario, cuentas administrativas, y/o de servicios (para el funcionamiento de sistemas operativos, bases de datos, etc.),
- asignación de accesos sobre la base de la necesidad de uso y el mínimo privilegio, que permita que el usuario cumpla con su rol funcional,
- definición de un período de vigencia para cada cuenta y sus privilegios asignados, en base a la utilización que se le dará a los mismos.

8.2.2.2 Casos especiales: Cuentas Administrativas

Estas cuentas están dotadas de un nivel superior de privilegios. Se emplearán exclusivamente para casos de administración de recursos, no siendo recomendable su uso habitual. De ser posible, existirán cuentas de usuario con menores privilegios, a ser empleadas por los administradores cuando no se requieran efectuar tareas especiales.

Las contraseñas de estas cuentas deberán tener mayor grado de complejidad.

El Responsable de Seguridad de la Información definirá procedimientos para la administración de dichas cuentas, siendo éstos implementados por el Responsable de Informática. Se contemplará lo siguiente, cuando corresponda:

- justificación formal de uso, determinación de los niveles de autorización requeridos,

- registro de actividades,
- renovación de contraseñas con mayor frecuencia.

8.2.2.3 Casos especiales: Cuentas Genéricas

Las cuentas genéricas se utilizarán para casos donde sea necesario identificar un área, en lugar de una persona física, p. ej.: cuentas de correo que identifican áreas que intervienen en procesos sustantivos del MTEySS.

El Responsable Primario deberá justificar su creación y uso. Se definirá un titular, quien será responsable por el uso de dicha cuenta. Asimismo, se detallará a las personas a las que se autorice su uso.

8.2.2.4 Casos especiales: Cuentas de Aplicativos y/o Servicios

Se trata de cuentas internas, generadas durante la instalación de servicios informáticos, y permiten, generalmente, acceso directo a datos. Entre las mismas, se encuentran las siguientes: *admin* (para la gestión de motores de bases de datos), administrador (cuenta básica de los sistemas operativos Windows) y *root* (cuenta básica de los sistemas operativos Linux).

El Responsable de Informática deberá implementar procedimientos que contemplen el cambio de nombre de dichas cuentas, la asignación de contraseñas complejas y la documentación segura de las mismas, prohibiéndose, por otra parte, el uso de estas cuentas por parte de usuarios a todo nivel.

8.2.3 Control: Gestión de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- los usuarios se comprometerán a mantener en secreto las contraseñas de sus cuentas. Esta declaración se incluirá en el Compromiso de Confidencialidad,
- se establecerá el empleo de contraseñas provisorias, asignadas a los usuarios cuando entran por primera vez al sistema, u olvidan su contraseña personal Las mismas sólo se ingresarán cuando el sistema haya acreditado la identidad del usuario,
- se obligará a que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema,
- la entrega de la contraseña provisoria o inicial al usuario se hará en forma personal, prohibiéndose la participación de ajenos, debiéndose verificar un acuse de recepción por parte de dicho usuario,
- se deberán cumplir pautas de complejidad, así como de renovación periódica de las contraseñas. Los Responsables de Seguridad de la Información y de Informática definirán, implementarán y verificarán el funcionamiento de estas políticas,
- se establecerán políticas que inhiban la reutilización de determinado número de contraseñas antiguas,
- las cuentas que acceden a múltiples servicios (*single sign on*) deberán tener contraseñas razonablemente complejas,
- las contraseñas se almacenarán en forma codificada, y en sistemas informáticos protegidos (p. ej.: utilizando *Active Directory* de *Windows*)
- se utilizarán tecnologías especiales, p. ej.: biometría, de requerirse. El Responsable de Informática, además del Responsable Primario, definirán y justificarán su uso, basándose en un análisis de riesgos.

8.2.4 Control: Administración de Contraseñas Críticas

Son contraseñas críticas aquellas correspondientes a cuentas administrativas y de servicio, mediante las que se efectúan actividades críticas como p. ej . instalación de plataformas o

sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc (ver *Capítulo 8.2.2 Control: Gestión de Privilegios*)

El Responsable de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas, contemplando lo siguiente:

- las contraseñas seleccionadas tendrán alto grado de complejidad,
- las contraseñas, así como la identificación de las cuentas a las que pertenecen se resguardarán en altas condiciones de seguridad,
- se dispondrá de un registro de uso y gestión de las contraseñas críticas, donde se indicarán las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con las mismas. El Responsable de Seguridad de la Información, en conjunto con el Responsable de Informática, efectuará una revisión periódica de dicho registro,
- donde sea posible, verificar que cada contraseña crítica se renueve una vez utilizada, o luego de un período establecido por el Responsable de Seguridad de la Información junto con el Responsable de Informática.

8.2.5 Control: Revisión de Derechos de Acceso de Usuarios

El Responsable de Seguridad de la Información, conjuntamente con los Responsables Primario y de Informática, mantendrá un control sobre el acceso a los datos y servicios de información.

A tal efecto, se llevará a cabo un proceso formal de revisión de los derechos de acceso de los usuarios. Se deben contemplar los siguientes controles:

- revisar los derechos de acceso de los usuarios a intervalos no mayores a 6 meses,
- revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos no mayores a 3 meses,
- revisar las asignaciones de privilegios a intervalos no mayores a 6 meses.

8.3 Categoría: Responsabilidades del Usuario

Objetivo

Se debe evitar el acceso de usuarios no autorizados, mitigando el riesgo de robo de información y/o de los medios de procesamiento, así como de modificaciones no autorizadas además de maniobras dolosas

Un esquema de seguridad efectivo debe contar con la cooperación de los usuarios autorizados. A través de actividades de concientización, se logrará clarificar las responsabilidades con relación al uso de claves y la seguridad de los puestos de trabajo, así como del cumplimiento de las políticas de escritorio y pantalla limpios (ver *capítulo 6.2.8 Controles: Políticas de Escritorios y Pantallas Limpias*).

8.3.1 Control: Uso de Contraseñas

Las contraseñas son un medio de validación y autenticación de la identidad de un usuario, así como la llave para acceder a las instalaciones de procesamiento de información.

Por lo anterior, se deben seguir buenas prácticas de seguridad en la selección y el uso de contraseñas, cumpliendo las siguientes directivas:

- mantener las contraseñas en secreto,
- pedir un cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las mismas contraseñas,
- seleccionar contraseñas complejas, de acuerdo con las políticas establecidas al respecto Tener en cuenta que las mismas:
  - no deben estar registradas en lugares de fácil acceso Se recomienda que sean fáciles de recordar,

- no deben basarse en datos que un ajeno pueda deducir fácilmente, p. ej.: no utilizar nombres de personajes populares, números de teléfono, fechas de nacimiento verificables, etc.,
- no deben tener caracteres o números idénticos consecutivos, así como secuencias de letras y números fácilmente deducibles

- cambiar las contraseñas cada vez que el sistema lo solicite, evitando su repetición según lo establecido (ver *capítulo 8.2.3 Control: Gestión de Contraseñas de Usuario*),
- los procesos automatizados evitarán la inclusión de contraseñas en las sesiones de inicio, p. ej.: aquellas almacenadas en una tecla de función o macro,
- notificar de acuerdo a lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad (ver *capítulo 11 Gestión de Incidentes de Seguridad*),

8.3.2 Control: Equipos Desatendidos en Áreas de Usuarios

Los equipos informáticos instalados en áreas de usuarios requieren protecciones específicas contra accesos no autorizados, especialmente cuando se encuentran desatendidos.

El Responsable de Seguridad de la Información coordinará con el Responsable de Recursos Humanos las tareas de concientización a usuarios internos, organizaciones externas y/o contratistas, donde corresponda, en lo referente a los requerimientos y procedimientos de seguridad para proteger equipos desatendidos.

El Responsable de Informática implementará políticas para el bloqueo, con re habilitación por contraseña, para todo el equipamiento instalado en las áreas de usuario. Se impedirá que los usuarios modifiquen dicha política, a menos que se autorice una excepción al respecto.

Los usuarios deberán concluir o bloquear manualmente las sesiones activas al finalizar las tareas o al retirarse del ámbito laboral, aun cuando esté activada la política de bloqueo.

8.4 Categoría: Control de Acceso a la Red

Objetivo

Controlar el acceso a los servicios de redes internas y externas controlados por el MTEySS, a fin de evitar accesos no autorizados y un posible compromiso sobre la información.

Se deberá asegurar:

- que existan interfaces apropiadas para interconectar la red del MTEySS, redes de otras organizaciones, y redes públicas,
- que se apliquen mecanismos de autenticación apropiados para la seguridad de los datos del MTEySS,
- que los controles para el acceso del usuario a la información del MTEySS sea obligatorio.

8.4.1 Control: Política de Utilización de los Servicios de Red

Se controlará el empleo de los servicios de red tanto internos como externos a fin de garantizar que los usuarios tengan un acceso tal que no comprometan la seguridad del MTEySS.

Se deberán priorizar las conexiones y aplicaciones críticas, y los accesos a sitios potencialmente inseguros, tales como áreas públicas y/o externas, instalaciones en la nube y las que se hallen fuera de la administración y el control directo del MTEySS.

Los Responsables de Seguridad de la Información y de Informática verificarán y otorgarán el acceso a los servicios y recursos de red, únicamente cuando se cumpla lo establecido en los procedimientos formales, en común acuerdo con los Responsables Primarios de la información del MTEySS.

Los procedimientos para implementar o inhibir los derechos de acceso a las redes contemplarán:

- la identificación de las redes y servicios para los cuales se requiere el acceso,
- la identificación de las personas y sus roles, para definir adecuadamente el modo de acceso a las redes y servicios,
- establecer procedimientos y controles de gestión para proteger el acceso a las conexiones y servicios de red.

8.4.2 Control: Camino Forzado

Las redes están diseñadas para permitir, en forma automática, el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta de comunicaciones a utilizar. Sin embargo, estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones o para el uso no autorizado de los recursos informáticos del MTEySS.

Por tal motivo, se establecerán límites para las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales éste requiera acceder.

El Responsable de Seguridad de la Información, conjuntamente con el Responsable de Informática y el Responsable Primario pertinente, realizarán una evaluación de riesgos a fin de determinar los mecanismos de control que correspondan en cada caso.

Se enumeran, a continuación, algunos de los controles a implementar:

- asignación de líneas telefónicas en forma dedicada, o con designación de responsable,
- conexión automática de puertos a pasarelas de seguridad (*gateways*) o a sistemas de aplicación específicos preestablecidos,
- imposición del uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.
- implementación de opciones de menú y submenú limitadas, en las aplicaciones, a los perfiles de los usuarios,
- limitación de la navegación ilimitada por la red, estableciendo dominios lógicos separados, p ej.: redes de área local virtuales, para grupos de usuarios definidos,
- control activo de las comunicaciones con origen y destino autorizados a través de gateways, y con generación de alertas ante eventos no previstos.

8.4.3 Control: Autenticación de Usuarios para Conexiones Externas

Se establecerán procedimientos de autenticación adecuados al nivel de protección requerido para los usuarios remotos.

El Responsable de Seguridad de la Información, conjuntamente con el Responsable Primario que corresponda, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación para conexiones externas, que corresponda en cada caso. El Responsable de Informática implementará los mecanismos establecidos, junto con el Responsable de Seguridad Física, cuando se requiera.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

- métodos de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
  - la herramienta de autenticación, conocida como autenticador,
  - el registro de los poseedores del dispositivo de autenticación,
  - la operatoria de devolución al momento de desvinculación del personal poseedor de un dispositivo,
  - método de revocación de acceso del autenticador, en caso de compromiso de seguridad,

- el protocolo de autenticación (p. ej.: desafío/respuesta), con un procedimiento que incluya:
  - establecimiento de las reglas, con el usuario,
  - establecimiento de un ciclo de vida de las reglas, para su renovación,
- utilización de líneas dedicadas, o herramientas de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión, donde sea pertinente,
- bloqueo de puertos para inhibir comunicaciones no autorizadas, especialmente sobre los sistemas de Voz sobre IP,
- procedimientos y controles de rellamada (*dial-back*), verificando que el desvío de llamadas, esté deshabilitado.

8.4.4 Control: Autenticación de Nodos

Se deberá emplear un esquema de identificación automática del equipamiento que se conecte a la red, sea en forma local a la red de datos, o cuando se trate de conexiones externas. La debida autenticación de los nodos de red evitará accesos no autorizados a las aplicaciones del MTEySS.

La autenticación de nodos será la alternativa, además, para verificar la identidad de usuarios locales y remotos, cuando éstos inicien una conexión a un servicio informático del Organismo.

Los dispositivos de autenticación deberán estar dotados de protecciones físicas (ver *6.1 Categoría: Áreas Seguras)*.

8.4.5 Control: Protección de los Puertos de Diagnóstico Remoto

Los puertos de diagnóstico remoto deben controlarse, para evitar que se los aproveche como medio de acceso no autorizado.

El Responsable de Informática generará acuerdos con el proveedor, a los fines de generar el marco de protección para la comunicación de los sistemas de diagnóstico remoto. Asimismo, los mecanismos de protección observarán lo establecido en los puntos *8.4.3 Control: Autenticación de Usuarios para Conexiones Externas* y *8.4.2 Control: Camino Forzado*.

8.4.6 Control: Subdivisión de Redes

La seguridad en redes extensas puede controlarse a través de una subdivisión en dominios lógicos, subredes o perímetros de seguridad separados, por medio de gateways con funcionalidades de firewall, estableciéndose redes locales virtuales (VLANs).

Para la subdivisión se tomarán en cuenta criterios de seguridad comunes a grupos de usuarios de red determinados. Asimismo, se considerarán aspectos como la exposición a amenazas comunes, las separaciones físicas y la segregación de tareas, cuando corresponda.

El Responsable de Informática se basará en un análisis de riesgos y en lo establecido en el punto ver *8.1 Categoría: Requerimientos para el Control de Acceso*, a los fines de evaluar costos relativos y el impacto en el desempeño de la red en general, cuando se introducen los enrutadores o gateways adecuados para subdividir la red. La decisión final sobre el esquema más apropiado a implementar será tomada junto con el Responsable de Seguridad de la Información.

8.4.7 Control: Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados para dar apoyo a la gestión del MTEySS.

El Responsable de Seguridad de la Información definirá los procedimientos para establecer el acceso a Internet, estableciendo las pautas de uso adecuadas a los recursos del MTEySS p. ej.: horarios de conexión, priorización de conexiones, servicios habilitados, etc.)

Los Responsables Primarios aprobarán la solicitud formal efectuada por el personal a su cargo. Los accesos autorizados serán implementados por el Responsable de Informática.

El Responsable de Seguridad de la Información verificará la actividad de los accesos, con el fin de evaluar la eficacia del servicio y el uso acorde a lo requerido. Asimismo, el Responsable de Informática implementará la instalación de firewalls y demás dispositivos que permitan efectivizar dichos controles.

Se comunicará a los usuarios los controles que se están ejerciendo sobre los accesos.

8.4.8 Control: Conexión a la Red

Sobre la base de lo definido en el *punto 8.1 Categoría: Requerimientos para el Control de Acceso, 8.4.2 Control; Camino Forzado* y *8.4.6 Control; Subdivisión de redes*, se implementarán controles para limitar a lo necesario la capacidad de conexión de los usuarios.

Ejemplos de los entornos donde deben implementarse restricciones son:

- correo electrónico,
- sistemas de archivos compartidos,
- accesos interactivos,
- accesos a la red fuera del horario o el ámbito laboral.

8.4.9 Control: Ruteo de Red

En las redes compartidas o que se extienden fuera de los límites del MTEySS se instalarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen las políticas de accesos establecidas.

Como mínimo, estos controles contemplarán la verificación positiva de direcciones de origen y destino, utilizando métodos tales como: la autenticación de protocolos de ruteo, el ruteo estático, la traducción de direcciones y las listas de control de acceso.

8.4.10 Control: Seguridad de los Servicios de Red

El Responsable de Seguridad de la Información, junto con el Responsable de Informática, definirá las pautas para garantizar la seguridad de los servicios de red, tanto públicos como privados, del MTEySS,

Se tendrán en cuenta las siguientes directivas:

- habilitar sólo aquellos servicios que sean requeridos en función de los procedimientos de autorización establecidos,
- controlar el acceso lógico a los servicios, tanto en lo referente a su uso como a su administración,
- efectuar un análisis de riesgos y vulnerabilidades para cada servicio, antes de habilitarlo,
- instalar periódicamente las actualizaciones de seguridad que requieran los dispositivos y los sistemas operativos,
- efectuar revisiones periódicas de las configuraciones.

8.5 Categoría: Control de Acceso al Sistema Operativo

Objetivo

Se deben utilizar medios de seguridad para restringir el acceso no autorizado a los sistemas operativos.

El Responsable de Seguridad de la Información y el Responsable de Informática realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso a los sistemas operativos del equipamiento informático, considerando tanto terminales de usuario como servidores de red.

Debe disponerse de procesos y controles que permitan implementar las siguientes acciones:

- autenticar a los usuarios autorizados, según la política de control de acceso establecida,
- registrar los intentos exitosos y fallidos de autenticación del sistema,
- registrar el uso de los privilegios especiales del sistema,
- emitir alarmas cuando se violan las políticas de seguridad del sistema,
- proporcionar los medios de autenticación apropiados,
- restringir el tiempo de conexión de los usuarios.

8.5.1 Control: Identificación Automática de Terminales

Se deberá implementar un proceso automatizado para la identificación de puestos de trabajo y servidores de procesamiento.

El proceso deberá proporcionar la siguiente información:

- el método de identificación de equipos utilizado,
- el detalle de transacciones permitidas por dispositivo.

8.5.2 Control: Procedimientos de Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro, de tal manera de minimizar la oportunidad de acceso no autorizado.

Se debe brindar la mínima información posible acerca del sistema, durante la conexión, para evitar que un usuario no autorizado reciba asistencia innecesaria.

En la conexión deben considerarse los siguientes factores:

- mantener en secreto los identificadores de sistemas y/o aplicaciones existentes, sólo divulgándolos después que el inicio de sesión haya concluido en forma exitosa,
- desplegar un aviso indicando que sólo pueden acceder a la computadora los usuarios autorizados,
- inhibir la emisión de mensajes de ayuda durante el procedimiento de conexión.
- validar la información de la conexión sólo cuando haya finalizado el inicio de sesión,
- evitar brindar información al usuario, en caso de aparecer una condición de error durante la conexión,
- limitar el número permitido de intentos de conexión no exitosos, teniéndose en cuenta lo siguiente:
  - llevar un registro de intentos no exitosos,
  - impedir intentos de conexión superado el límite permitido,
- limitar el período de tiempo en el cual es posible efectuar la conexión. Fuera de ese lapso, se debe deshabilitar la conectividad,
- permitir el despliegue de los siguientes datos, cuando se verifique el inicio de sesión:
  - fecha y hora de la conexión exitosa anterior,
  - detalle de los intentos de conexión no exitosos posteriores al último inicio de sesión.

8.5.3 Control: Identificación y Autenticación de los Usuarios

Todos los usuarios de la red del MTEySS, -incluyendo al personal técnico, administradores, programadores y desarrolladores- tendrán una cuenta única de acceso a los recursos, individualizada con un identificador, conocido como ID de usuario.

El ID de usuario será unívocamente asociado a una cuenta, de manera de garantizar la trazabilidad individual de las acciones sobre los recursos.

Las reglas de creación de las cuentas deben considerar que el ID de usuario no podrá brindar ningún indicio del nivel de privilegio otorgado.

Podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica, p. ej.: cuentas genéricas de correo o cuentas grupales de red (ver *Capítulo 8.2.2 Control: Gestión de Privilegios*).

Para casos donde se requiera un control especial de autenticación de origen y verificación de integridad, p. ej.: firma digital, se utilizarán autenticadores de hardware físicos –tokens-, debiendo cumplirse lo indicado en el punto *8.4 3 Control: Autenticación de Usuarios para Conexiones Externas*.

8.5.4 Control: Sistema de Administración de Contraseñas

El sistema de gestión de contraseñas garantizará el cumplimiento de las políticas de seguridad establecidas para las cuentas de los usuarios y sus accesos a los recursos del MTEySS.

El sistema dispondrá de una gestión centralizada. Se permitirá que los usuarios elijan y cambien sus propias contraseñas, ajustándose a lo indicado lo indicado a los puntos *8.3.1 Control: Uso de Contraseñas* y *8.2.3 Control: Gestión de Contraseñas de Usuario.*

Se implementarán los controles que se detallan a continuación:

- políticas obligatorias de complejidad en la definición de una contraseña, p. ej.: una contraseña deberá contener letras y números, un carácter especial y dos letras en mayúscula,
- longitud mínima de una contraseña, p. ej.: contener 8 caracteres o más,
- procedimientos para generar y entregar en forma segura la contraseña inicial,
- plazo obligatorio para que los usuarios modifiquen la contraseña, p. ej.: modificar las contraseñas cada 42 días,
- prohibición de reutilizar determinado número de contraseñas, cuando se las renueve, p ej.: no repetir las últimas 13 contraseñas,
- inhibición del despliegue en pantalla de las contraseñas, cuando están siendo ingresadas, p. ej.: mostrar asteriscos en el campo donde se tipea la contraseña,
- almacenamiento de los archivos de las contraseñas en forma cifrada, ubicados en entornos separados respecto de los archivos de datos de los sistemas, con un nivel de máxima seguridad física y lógica,
- obligación de modificar las cuentas y contraseñas predeterminadas (*built in*) por el proveedor, debiendo tener el mayor nivel de complejidad que el establecido de fábrica.

8.5.5 Control: Uso de Utilitarios de Sistema

Los utilitarios de sistema suelen utilizarse para operaciones de soporte y/o administración de la plataforma informática. Dado que tienen la capacidad para pasar por alto verificaciones de seguridad, es necesario que su uso se encuentre restringido y minuciosamente controlado.

Se deben considerar los siguientes controles:

- procedimientos de autenticación para utilitarios del sistema,
- separar utilitarios del sistema y software de aplicaciones en entornos distintos,
- restringir el uso de utilitarios del sistema a la cantidad mínima justificable de personal autorizado, p. ej : sólo a administradores de dominio e implementadores,
- definir y documentar los niveles de autorización requeridos para acceder a los utilitarios del sistema,
- evitar que personas ajenas al MTEySS tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas,

- registrar el uso de utilitarios del sistema,
- eliminar los utilitarios del sistema de las instalaciones de usuario final.

8.5.6 Control: Alarmas Silenciosas para la Protección de los Usuarios

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción.

Se tomará como base la realización de una evaluación de riesgos, a cargo del Responsable de Seguridad de la Información junto con los Responsables Primarios, de Informática, Recursos Humanos y/o Seguridad Física, cuando corresponda.

Asimismo, se definirán y asignarán funciones y procedimientos para responder a la utilización de una alarma silenciosa.

8.5.7 Control: Desconexión de Terminales por Tiempo Muerto

Los puestos de trabajo deberán contar con una protección por desconexión luego de un período de inactividad, teniendo en cuenta lo establecido en el punto 6.2.8 *Controles: Políticas Escritorios y Pantallas Limpias*.

El apagado se efectuará luego de un período de inactividad –llamado también tiempo muerto-, habilitándose un protector de pantalla resguardado con contraseña.

El lapso por tiempo muerto será fijado por el Responsable de Seguridad de la Información, junto con el Responsable de Informática, en forma global para todas las sesiones iniciadas sobre la red de datos del MTEySS.

Asimismo, el usuario deberá activar manualmente el protector cuando abandone su ámbito de trabajo, especialmente en zonas de acceso público.

8.5.8 Control: Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a los sistemas y aplicaciones del MTEySS, ya que permiten reducir el espectro de oportunidades para el acceso no autorizado.

El Responsable Primario definirá el límite de horario de conexión a los recursos informáticos asignados, en forma adecuada a la operatoria del área bajo su cargo, gestionando asimismo las excepciones o cambios. El Responsable de Informática efectuará la implementación de este control.

Entre los controles que se deben aplicar, se distinguen:

- limitar los tiempos de conexión al horario normal de oficina,
- justificación formal de cambios o excepciones, p. ej.: cuestiones operativas o actividades críticas).

8.6 Categoría: Control de Acceso a las Aplicaciones

Objetivo

Se restringirá el acceso a los sistemas de aplicación a los fines de proteger la información contra operaciones no autorizadas.

Los controles en los sistemas de aplicación deben tener en cuenta lo siguiente:

- se establecerán protecciones para evitar accesos no autorizados por parte de personas, software no relacionado y/o malicioso,
- se establecerán los roles mínimos y necesarios para que las aplicaciones cumplan con la funcionalidad para la que fueron diseñadas,
- el acceso a las operaciones será a través de menús e interfaces adecuadas, impidiéndose una operación directa sobre los datos,

- se asegurará la no interferencia en la funcionalidad individual de los sistemas que se encuentren intercomunicados.

8.6.1 Control: Restricción del Acceso a la Información

El acceso a la información estará basado en lo establecido en el punto *8.2.2 Control: Gestión de Privilegios*, de manera que se eviten riesgos por daños, pérdidas o modificaciones no autorizadas.

8.6.1.1 Responsabilidades en el Acceso a la Información

El Responsable de Informática implementará, configurará y administrará las interfaces y el control de accesos a los aplicativos.

Asimismo, el Responsable Primario autorizará los requerimientos formales de acceso a las funciones de cada aplicativo. Asimismo, se establecerá un procedimiento para delegar la administración de los accesos en los Responsables Primarios que hagan uso de una aplicación en particular.

Las operaciones técnicas y de soporte informático de los sistemas serán efectuadas por personal autorizado, a cargo del Responsable de Informática, con una aprobación formal del Responsable Primario que corresponda.

Las verificaciones y operaciones de monitoreo de seguridad serán llevadas a cabo por el Responsable de Seguridad de la Información, junto con el Responsable de Informática, donde corresponda, con una aprobación formal del Responsable Primario competente.

Las excepciones, serán informadas al Responsable Primario y a la Unidad de Auditoría Interna, estableciéndose procedimientos de autorización, registración y auditorías adecuados.

8.6.1.2 Restricciones al acceso a la Información

Se aplicarán los siguientes controles que brinden apoyo a los requerimientos de limitación de accesos:

- el conocimiento de los usuarios acerca de la información o de las funciones y la documentación de los sistemas se restringirá a las operaciones para las cuales se hallen autorizados,
- se controlarán los derechos de acceso de los usuarios a las operaciones, p. ej.: lectura, escritura, eliminación y ejecución,
- las salidas de datos de los sistemas de aplicación (listados, informes, etc.) sólo contendrán la información específica requerida por la entrada,
- las salidas se publicarán y/o enviarán únicamente a puestos, impresoras, sitios web, etc., que se hallen autorizados,
- las salidas de datos deberán revisarse periódicamente, a fin de detectar y eliminar información redundante.

8.6.1.3 Aspectos de administración

Para poder administrar adecuadamente las limitaciones de acceso, se considerarán los siguientes aspectos:

- el acceso a los sistemas se realizará a través de interfaces de usuario (camino forzado),
- se evitará la posibilidad de procesar datos ya sea en forma directa sobre las bases, o por fuera de las interfaces de usuario. Estas opciones sólo se justificarán, cuando se trate de ambientes de desarrollo o pruebas especiales,
- los privilegios de control pleno (*full control*) serán asignados exclusivamente a los administradores de los servicios que corresponda, observando el principio de segregación de tareas. P ej.: el administrador de bases de datos no accederá a la administración de las comunicaciones,

- El Responsable de Seguridad de la Información, y quien éste designe, tendrán privilegios de plena visibilidad, sin modificación (*read only*), sobre todos los objetos de información y de la instalación.

8.6.2 Control: Aislamiento de los Sistemas Sensibles

Los sistemas y aplicativos del MTEySS deben ejecutarse en ambientes controlados, considerando las siguientes configuraciones:

- instalación en procesadores dedicados,
- instalación compartida sólo con otros sistemas confiables,
- instalación compartida sin límite.

El Responsable Primario deberá indicar el nivel de sensibilidad y/o criticidad con el que el sistema está clasificado (ver *Capítulo 4.2 Clasificación de la Información*).

Son aplicables las siguientes consideraciones:

- según el nivel de clasificación, se acordará la configuración adecuada para los entornos del sistema que procese los datos. Esta tarea la efectuarán los Responsables de Seguridad de la Información y de Informática, con el Responsable Primario,
- el Responsable Primario determinará con el Responsable de Informática la disponibilidad requerida para los servicios en el entorno donde se ejecutará la aplicación, basándose en las necesidades de operación y seguridad,
- se evaluarán métodos para compartir la información, p. ej.: sistemas de archivos, sistemas clientes/servidor, portales de Intranet/Internet, etc.,
- se deberá definir el nivel de seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones,
- el Responsable de Seguridad de la Información, junto con el Responsable de Informática analizará las protecciones de seguridad necesarias, en el marco de un plan de continuidad y/o contingencia para los sistemas. P. ej.: la determinación del equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

8.7 Categoría: Monitoreo del Acceso y Uso de los Sistemas

Objetivo

Teniendo en cuenta factores como la criticidad y el uso de la información involucrada, la interoperabilidad de los sistemas y la posibilidad de ataques, se buscan los siguientes objetivos:

- asegurar que se registren y se evalúen todos los eventos significativos para la seguridad de accesos,
- verificar la existencia de procedimientos para monitorear el uso de las instalaciones de procesamiento de la información.

8.7.1 Control: Registro de Eventos

Los registros de auditoría deberán incluir eventos relativos a la seguridad y excepciones, tales como:

- identificación del usuario y el puesto de trabajo,
- fecha y hora de inicio, terminación de las conexiones de red,
- sistemas y/o aplicativos, intentos de acceso al sistema, exitosos y fallidos,
- excepciones de los sistemas de registro, alarmas de administración de redes,
- acceso remoto.

Los Responsables de Informática y de Seguridad de la Información, junto con la Unidad de Auditoría Interna, definirán un cronograma de depuración de registros en línea, según las normas vigentes y los requerimientos operativos del MTEySS.

8.7.2 Control: Monitoreo en Áreas Protegidas

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información del MTEySS, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Los usuarios deberán conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo (ver *Capítulo 5.2.4 Control: Compromiso de Confidencialidad y Uso Adecuado de los recursos de información* y *7.10 Categoría: Seguimiento y Control)*.

8.7.2.1 Responsabilidades

Los Responsables Primarios indicarán los requerimientos para registrar aquellos eventos que consideren críticos para la operatoria en las áreas bajo su cargo.

Por su parte, el Responsable de Informática efectuará una evaluación de riesgos a fin de determinar el alcance de los procedimientos de registración.

8.7.2.2 Factores de Riesgo en las áreas

Entre los factores de riesgo que se deben considerar se encuentran:

- la criticidad de los sistemas,
- el valor, la sensibilidad y la criticidad de la información involucrada,
- la posibilidad de ataques, filtraciones o uso inadecuado del sistema,
- la interoperabilidad y la conexión entre los sistemas.

8.7.2.3 Eventos a verificar en las áreas de riesgo

Entre los eventos a tener en cuenta se enumeran las siguientes:

- acceso no autorizado, incluyendo detalles como:
  - identificación del usuario,
  - fecha y hora de eventos clave,
  - tipos de evento,
  - archivos a los que se accede,
  - utilitarios y programas utilizados,
- todas las operaciones privilegiadas, como:
  - utilización de cuentas administrativas o con permisos especiales,
  - inicio y cierre del sistema,
  - conexión/desconexión de dispositivos de transferencia y/o copia de datos,
  - intentos de cambio de fecha y hora,
  - cambios en la configuración de la seguridad,
  - alta o baja de servicios,
- intentos de acceso no autorizado, como:
  - intentos fallidos,
  - violaciones a las políticas de acceso
  - notificaciones de firewalls y dispositivos de red,

- alertas de sistemas de detección de intrusiones,

- alertas o fallas de sistema, como:
  - alertas o mensajes de consola,
  - excepciones del sistema de registro,
  - alarmas del sistema de administración de redes,
  - accesos remotos a los sistemas.

8.7.3 Control: Registro y Revisión de Eventos

Se implementará un procedimiento de registro y revisión de los registros de auditoría, con el fin de producir reportes de amenazas detectadas, los métodos de ataque utilizados y las formas de mitigarlos.

El Responsable de Seguridad de la Información, el Responsable de Informática y los Responsables Primarios determinarán la periodicidad para efectuar las revisiones, tomando como base una evaluación de riesgos.

De acuerdo a lo establecido en el *Control: 2.2.1 Asignación de responsabilidades*, se debe separar las funciones de revisión respecto de las actividades que se monitorean.

El Responsable de Informática dispondrá la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control unificado de los registros, cuando se requiera.

La Unidad de Auditoría Interna tendrá acceso de consulta sobre los registros de eventos, con el fin de colaborar en el control, evaluar las herramientas de registro y recomendar modificaciones a los aspectos de seguridad.

Se dispondrá, en caso de ser necesario, de archivos auxiliares, a fin de copiar sobre ellos los registros más significativos, cuando el volumen de información del registro principal sea muy grande.

Las herramientas dispondrán de los controles de acceso necesarios, para evitar lo siguiente:

- la desactivación de la herramienta de registro,
- la alteración de mensajes registrados,
- la edición o supresión de los archivos de registro,
- la saturación de un medio de soporte de archivos de registro,
- fallas en los registros de eventos,
- la sobreescritura de los registros.

8.8 Categoría: Dispositivos Móviles y Trabajo Remoto

Objetivo

Asegurar la seguridad de la información cuando se utilizan medios de computación móviles y el esquema de trabajo remoto o teletrabajo.

8.8.1 Control: Computación Móvil

La protección de las soluciones móviles debe comenzar por la definición taxativa de políticas de uso dentro del MTEySS, teniendo en consideración los riesgos que implica el trabajar en un ambiente sin protección, de forma de garantizar un marco seguro para la información del Organismo.

En el *Capítulo 7.7.1 Control: Administración de Medios Informáticos Removibles* se indica un breve resumen de los dispositivos móviles más utilizados en la actualidad.

En el caso de teléfonos inteligentes y recursos de almacenamiento, debe establecerse quién es el dueño de los dispositivos, quién puede almacenar sistemas o datos del MTEySS, y quién es el Responsable Primario de los mismos.

8.8.1.1 Responsabilidades

El Responsable de Seguridad de la Información confeccionará una lista de dispositivos móviles, considerando los riesgos para cada caso y estableciendo los controles de seguridad pertinentes.

El Comité de Seguridad de la Información verificará los controles propuestos, efectuando las recomendaciones que correspondan.

Los Responsables de Informática y de Seguridad Física implementarán los controles que correspondan.

8.8.1.2 Consideraciones Generales

Los procesos de uso y control de los dispositivos móviles abarcarán los siguientes conceptos:

- análisis de los sistemas operativos utilizados por los dispositivos (p. ej.: tabletas, *netbooks*, *notebooks* y teléfonos inteligentes) y su estructura de seguridad,
- existencia de antivirus y otros sistemas de prevención de software malicioso,
- uso en lugares públicos,
- concientización a los usuarios,
- implementación de herramientas centralizadas para la gestión de seguridad, donde corresponda,
- mecanismos de protección física y acceso seguro a los dispositivos,
- restricciones para grabar información del MTEySS –donde corresponda-,
- monitoreo de dispositivos que se conectan a la red de datos del MTEySS,
- acceso a los sistemas y servicios del MTEySS a través de los dispositivos móviles,
- técnicas criptográficas a utilizar para la transmisión de información,
- mecanismos de resguardo de la información contenida en los dispositivos,
- procesos de retorno de aquellos dispositivos propiedad del MTEySS,
- rúbrica de Compromisos de Confidencialidad relacionados con el almacenamiento de información en los dispositivos,
- procedimientos de reporte y denuncia, en casos de robo o extravío,
- procedimientos de revocación de claves y eliminación remota de datos, cuando corresponda.

8.8.1.3 Concientización para el uso de dispositivos móviles

Se efectuarán las siguientes recomendaciones a seguir en cada caso:

- no dejar dispositivos o medios desatendidos,
- mantener precauciones de uso en lugares públicos,
- no llamar la atención (especialmente en el caso de dispositivos novedosos como teléfonos celulares 3G, dispositivos reproductores mp4, tabletas, etc.),
- cifrar la información clasificada.

8.8.2 Control: Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al MTEySS. Se considera que el trabajo remoto –o

teletrabajo-, es una extensión de los recursos informáticos de oficina ofrecidos por el MTEySS a sus usuarios.

En este esquema, deben establecerse controles adecuados para proteger los accesos, las comunicaciones y la operación sobre los datos del Organismo.

El trabajo remoto será autorizado y justificado por el Responsable Primario del área a la cual pertenezca el usuario solicitante. El acceso será otorgado por un período de tiempo, y podrá ser renovado, según corresponda.

El Responsable de Seguridad de la Información definirá los requisitos de acceso, así como los procedimientos de monitoreo y auditoría pertinentes.

Los accesos serán implementados por el Responsable de Informática, cuando se verifique que se cumplen las políticas de seguridad, normas y procedimientos existentes.

8.8.2.1 Pautas generales para el teletrabajo

Los procedimientos establecidos para el trabajo remoto tendrán en cuenta:

- seguridad física existente en el edificio y en el ambiente de la instalación remota,
- riesgos de utilización de la instalación remota por ajenos no autorizados,
- justificación del acceso remoto a los sistemas internos del Organismo,
- acceso permitido por un período definido, con renovación justificada por el Responsable Primario,
- homologación del software residente en el equipamiento remoto,
- análisis de la sensibilidad y/o criticidad de la información y los sistemas a acceder,
- análisis y autorizaciones de acceso a los recursos del MTEySS a utilizar, p. ej.: correo Web, redes privadas virtuales, recursos compartidos a acceder, transferencias mediante dispositivos móviles, etc.,
- análisis y mitigación de riesgos por accesos no autorizados,

8.8.2.2 Controles para el teletrabajo

Los controles y disposiciones comprenden:

- mobiliario para almacenamiento y equipos, adecuados a las actividades de trabajo remoto,
- tipo y horario de trabajo,
- sistemas y servicios autorizados al trabajador remoto,
- concientización sobre la seguridad física a observar en la instalación remota,
- auditorías y monitoreo de la seguridad sobre las conexiones a equipos remotos,
- bloqueos de acceso al finalizar las actividades de trabajo remoto,
- reintegro de equipamiento, cuando corresponda,
- renovación o anulación del acceso remoto, cuando corresponda.

8.8.3 Control: Acceso a los sistemas en la nube

La información del MTEySS que se almacene o procese bajo servicios de nube debe gozar de la misma protección o mayor que la establecida para el ámbito del Organismo (ver el *Capítulo 7.2.4 Control: Servicios en la nube*).

Los controles de seguridad de la información que se transferirán al proveedor deben basarse en una gestión de riesgos. Dichos controles estarán definidos por el Responsable de Seguridad de la Información, con un acuerdo de los Responsables Primarios que corresponda. La

implementación en la plataforma computacional será llevada a cabo por el Responsable de Informática.

8.8.3.1 Controles generales para las operaciones de los sistemas en la nube

Los procesos y las operaciones tendrán en cuenta lo siguiente:

- se identificarán las estructuras y los procesos colaborativos de control, a establecerse entre el MTEySS y el proveedor de los servicios de nube,
- se establecerán los requisitos de diseño, desarrollo y entrega de los servicios prestados por el proveedor, documentado dentro de un Acuerdo de Nivel de Servicios,
- se establecerán los procesos de disponibilidad, continuidad, eficiencia y seguridad del servicio implementado en la nube, se implementarán las técnicas de acceso a la nube adecuadas para el MTEySS,
- se establecerá un nivel de clasificación de los activos y la información a ubicar en la nube,
- se deberá determinar la ubicación física y/o lógica de los datos en la nube, en relación a las instalaciones del MTEySS,
- se establecerán tanto el alcance como las responsabilidades legales por incumplimiento de los acuerdos establecidos,
- las políticas de seguridad en la nube deberán tener un enfoque más restrictivo que el aplicado en las políticas de las sedes del MTEySS,
- se establecerán límites a los privilegios de acceso, basados en los requerimientos y necesidades de uso de la información, para los sistemas y la información que se halle en la nube,
- se implementará un esquema de administración de accesos de usuarios coordinada entre el proveedor de la nube y el MTEySS,
- el MTEySS se reservará el derecho a auditar al proveedor de servicios de nube, siguiendo lo establecido en la normativa legal vigente,
- el MTEySS verificará que los procedimientos para dar respuesta a incidentes que haya implementado el proveedor de servicios de nube sean los adecuados a la criticidad de la información allí procesada o almacenada,
- la planificación de continuidad deberá incluir lo relativo a casos de desastres, estableciéndose, una coordinación adecuada entre proveedor y el MTEySS,
- se deberá verificar que la transferencia de datos entre los servicios de la organización cliente y la nube se realice de forma segura, considerando una adecuada portabilidad, cifrado de los datos en tránsito y eliminación de datos y sus metadatos asociados, cuando se lo requiera.

9. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas

Generalidades

El desarrollo y mantenimiento de las aplicaciones son puntos críticos para la seguridad de la información del MTEySS.

Se deben aplicar controles que garanticen la protección de los datos, considerando todas las etapas del ciclo de vida de las aplicaciones.

Los requerimientos de seguridad deben identificarse y aprobarse durante la etapa de análisis y diseño, siendo desarrollados y testeados en la etapa de desarrollo y prueba. Finalmente, se los valida e implementa cuando el sistema es instalado en el ambiente de producción.

El conjunto de controles debe incluir procesos de validación de datos a la entrada, durante el procesamiento interno y a la salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas. Se debe evitar que el personal dedicado a desarrollo acceda a los sistemas y plataformas que se encuentran en los ambientes productivos, y, en casos excepcionales, se deberá establecer un proceso de registro y trazabilidad de acciones

Debe implementarse, por otra parte, una adecuada administración de la infraestructura de base (sistemas operativos, utilitarios, motores de bases de datos, plataformas de publicación) para los distintos entornos de trabajo (ver *Capítulo 7.1.4 Control: Separación entre las Instalaciones de Desarrollo, Prueba, Homologación y Producción*).

Objetivo

Los objetivos de esta cláusula son:

- asegurar la inclusión de controles de seguridad y validación de datos en los sistemas desarrollados por el MTEySS o en la adquisición de paquetes de software,
- definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y sobre la infraestructura de base en la cual se apoyan,
- definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos desarrollados en el MTEySS, cedidos por organizaciones externas o adquiridos a proveedores externos.

Quedan alcanzados, además, los sistemas operativos y software de base instalados en los ambientes de procesamiento administrados por el Organismo.

Responsabilidades

El Responsable de Seguridad de la Información, junto con el Responsable Primario y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente y en los paquetes de software de organizaciones externas y/o contratistas, en función de una evaluación previa de riesgos.

Por otro lado, el Responsable de Seguridad de la información, en acuerdo con el Responsable Primario, definirá e implementará los requerimientos de protección de los datos, tomando en consideración los niveles de clasificación definidos (ver *Capítulo 4.2 Categoría: Clasificación de la información*) y la aplicación de métodos criptográficos.

El Responsable de Seguridad de la Información cumplirá, asimismo, con las siguientes funciones:

- verificar el cumplimiento de los controles y requerimientos de seguridad establecidos para el desarrollo y el mantenimiento de los sistemas y los paquetes de software,