Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones

(MAAGTIC)

ANEXO

Proceso 5.9.4 ASSI: Administración de los sistemas informáticos

5.9.4.4 Reglas de Operación
1.6. Reglas mínimas que deberán ser observadas por las UTIC, relacionadas con la seguridad de la información contenida en medios electrónicos

SECRETARÍA DE LA FUNCIÓN PÚBLICA

Julio de 2010

Anexo al Proceso:	
5.9.4 ASSI	**Administración de la seguridad de los sistemas informáticos**
5.9.4.4	**Reglas de operación**
1.6	**Reglas mínimas que deberán ser observadas por las UTIC, relacionadas con la seguridad de la información, ordenadas por Objetivo de control según el marco ISO 270001**

A.5 Política de seguridad

1. Todo el personal de la dependencia o entidad está obligado a operar en un ambiente de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información, de acuerdo a las disposiciones de la presente norma.

2. Las reglas de operación de los procedimientos de seguridad de la información, deberán revisarse y actualizarse cuando cambien las condiciones de las soluciones tecnológicas o cuando cambie la legislación aplicable.

A.6 Organización de la seguridad de la información

1. El personal de la UTIC responsable de la seguridad de los recursos de TIC deberá certificar que el personal externo, que tenga cualquier tipo de contacto con recursos de TIC institucionales, cumpla con las disposiciones de este manual.

2. Las Instituciones no otorgarán el derecho de intercambio de información con entidades externas en caso de que los controles identificados por la UTIC en éstas últimas no cumplan satisfactoriamente con la prevención de los riesgos de integridad y confidencialidad de la información de la dependencia o entidad.

3. Se permitirá al personal de los proveedores de servicios el acceso a los puntos de red únicamente con la autorización del responsable del proyecto o proceso en el que trabaje ese personal.

4. El personal de la UTIC con atribuciones para ello será responsable de autorizar los accesos del personal de los proveedores de servicios y del registro correspondiente.

A.7 Administración de activos

1. Los propietarios de la información son los responsables de la custodia y buen uso de la información que se almacena, procesa y transmite dentro de las Instituciones.

2. Los usuarios de TIC y, en particular los propietarios de la información almacenada en medios electrónicos, definirán los requerimientos de seguridad de su información y de sus sistemas de información.

3. La UTIC, en conjunto con los usuarios responsables de la información clasificada como confidencial o

reservada, determinará los esquemas de seguridad que se aplicarán para mantener su confidencialidad, disponibilidad e integridad.

4. La información clasificada según la LFTAIPG como confidencial o reservada deberá residir en territorio nacional. Los servicios de almacenamiento y administración de la misma deberán realizarse de igual manera dentro del territorio nacional.

5. Las UTIC y sus usuarios deberán apegarse al esquema de la APF para la clasificación de la información, a fin de definir sus niveles de protección.

6. La información que se genera, almacena, procesa y transmite por medios electrónicos será almacenada, resguardada y administrada por la UTIC en función de la clasificación indicada por los usuarios propietarios o responsables de ella, al momento de definir los requerimientos de las soluciones tecnológicas o servicios de TIC que se construyan para cada usuario.

7. Las UTIC y los usuarios involucrados deberán velar por que cada medio de almacenamiento desmontable o removible, con información clasificada como confidencial, reservada o pública, sea etiquetado por el responsable del mismo, de acuerdo a la normatividad vigente.

8. La UTIC, en conjunto con los usuarios de la información almacenada en medios electrónicos clasificada como confidencial o reservada, determinarán los esquemas de seguridad necesarios para mantener su confidencialidad, disponibilidad e integridad.

A.8 Seguridad de los recursos humanos

1. El usuario debe dar cumplimiento a todas las disposiciones que le sean comunicadas por la UTIC, tanto relacionadas con el uso de las soluciones tecnológicas, los servicios de tecnologías de la información, como de equipos PC. Debe también estar al tanto de sus responsabilidades, por lo que debe firmar, bajo protesta de decir verdad, que conoce las disposiciones, el inventario de software y hardware instalado en su equipo.

2. Las UTIC deberán fijar los mecanismos de seguridad de la información para el personal en aquellos cargos de la estructura organizacional de la UTIC donde se maneje información confidencial.

A.9 Seguridad física y ambiental

1. La UTIC deberá implementar mecanismos de control de acceso a las instalaciones del centro de datos, del centro de telecomunicaciones y de todas aquellas instalaciones en las que se encuentre equipo de almacenamiento, procesamiento y/o transmisión de información. La UTIC debe contar con mecanismos de control que permitan asegurar que el personal que ingrese a sus instalaciones cuente con la autorización correspondiente.

2. El personal de la UTIC que administre la infraestructura de TIC debe llevar un registro del personal y justificar el motivo de acceso a las áreas en las que se encuentran estos componentes. El registro de acceso deberá incluir datos que permitan la fácil localización del personal que ingresó a las áreas citadas.

3. El personal de la UTIC que administre la infraestructura de TIC debe mantener actualizadas las listas de autorización de acceso a personal de proveedores de servicios de terceros y llevar el control de accesos

presenciales y remotos indicados en el punto anterior.

4. Se permitirá al personal de los proveedores de servicios el acceso a los puntos de red -incluyendo el acceso a los nodos de la red de la dependencia o entidad- solo bajo la supervisión del responsable de las instalaciones físicas de TIC. El personal de los proveedores de servicios deberá presentar identificación oficial y de la empresa que representa al momento de solicitar el acceso.

5. El personal de la UTIC debe instalar la infraestructura de TIC en ambientes físicos adecuados para su operación, administración, monitoreo y control de acceso, para minimizar las riesgos, amenazas y condiciones de operación fuera de las especificaciones indicadas por los proveedores correspondientes.

6. Los usuarios de equipos de cómputo de escritorio deben asegurarse de utilizar y mantener cerradas las chapas de seguridad de estos equipos. Los usuarios de equipos portátiles deberán asegurarse de colocar el cable y candado de seguridad correspondientes.

7. Vía la mesa de servicios, el personal de la UTIC responsable de la seguridad de los recursos de TIC, se asegurará de que el equipo de escritorio, portátil, o de cualquier otro tipo, que utilizará la conexión a la red institucional se encuentre libre de virus informático.

8. La UTIC, siguiendo el proceso de Administración de la infraestructura física de TIC, deberá evaluar y certificar la seguridad de las instalaciones eléctricas, de comunicaciones, de sistemas contra incendios, de aire acondicionado y de otros recursos, que garanticen las condiciones adecuadas de seguridad para la operación de la infraestructura física de TIC de la dependencia o entidad.

9. Las UTIC deberán asegurar que los nodos de comunicaciones a las redes institucionales estén ubicados en lugares cerrados y resguardados

A.10 Gestión de las comunicaciones y operaciones

1. Vía la mesa de servicios, el personal responsable de la seguridad de los recursos de TIC se asegurará de que el equipo que utilizará la conexión a la red institucional se encuentre libre de virus informáticos, así como de lo necesario para mantener su seguridad y la de la red institucional.

2. Los usuarios y el área de soporte técnico de la UTIC de forma periódica (semestral, mensual, quincenal) deben realizar copias de seguridad de la información crítica que almacenen en su equipo.

3. La UTIC deberá solicitar por escrito a los usuarios responsables de los servicios, las necesidades de respaldo de sus datos. Estos deberán tomar en cuenta el tipo de información y las necesidades de operación de los propios servicios, en apego a la normatividad aplicable.

El área de la UTIC designada responsable de la ejecución de los respaldos deberá efectuarlos en estricto apego a los requerimientos indicados por los usuarios.

4. El área de la UTIC designada responsable deberá elaborar el calendario de respaldos y comunicarlo a la UTIC, considerando las necesidades de los usuarios responsables de los servicios, así como las necesidades de las soluciones tecnológicas y centro de datos de la UTIC.

5. El área de la UTIC designada responsable del calendario de respaldos deberá conservar evidencia del

respaldo efectuado y garantizar la integridad de la información.

6. El área de la UTIC designada responsable deberá mantener los controles necesarios para conocer el estado de cada copia de respaldo y su ubicación.

7. El área de la UTIC designada responsable deberá implantar procedimientos para preparar y almacenar la información y probar periódicamente la integridad de los respaldos.

8. El área de la UTIC designada responsable deberá mantener una copia del software, soluciones tecnológicas, aplicativos, parámetros de configuración de ambientes, estructuras de datos y datos; anterior a la versión en operación.

10. El área de la UTIC designada responsable deberá generar las copias necesarias de los respaldos y almacenarlas en inmuebles diferentes, a fin de garantizar la recuperación de la operación, en caso de ejecutarse algún plan de contingencia.

11. El área de la UTIC designada responsable deberá registrar en una bitácora de evidencias las recuperaciones realizadas, indicando al menos, el número de solicitud de la restauración, el dueño de la información, el nombre del sistema, la sección solicitada y el número de serie del respaldo utilizado.

12. El área de la UTIC designada responsable deberá atender solamente las solicitudes de restauración efectuadas por escrito; la solicitud deberá contener al menos: nombre y firma del propietario de la información, nombre del sistema del cual se desea recuperar la información, especificaciones de la información que se desea recuperar.

13. El área de la UTIC designada responsable en conjunto con las áreas propietarias de la información y/o las soluciones tecnológicas determinará la permanencia y la vigencia de la información respaldada , en concordancia con la legislación aplicable..

14. El área de la UTIC designada responsable deberá en conjunto con las áreas propietarias de la información, definir el mecanismo específico, por sistema o por tipo de información, de eliminación de respaldos.

15. Los usuarios que requieran conectarse a la red institucional utilizando equipo de cómputo de escritorio o portátil, propio o institucional, deberán obtener autorización de la UTIC vía la mesa de servicios, la cual será responsable de habilitar su conexión.

16. La información confidencial o reservada contenida en medios de almacenamiento bajo responsabilidad de la UTIC que vayan a dejar de usarse, deberán ser borrados mediante un medio que garantice la eliminación física total de la información. Deberá aplicarse también si van a ser reutilizados o entregados a un tercero para reparación o en préstamo. Deberá obtenerse una evidencia de la eliminación. Si los medios de almacenamiento de los equipos y accesorios están bajo el resguardo de los usuarios, estas acciones serán responsabilidad del usuario. En caso de requerirlo, podrán solicitar apoyo a la UTIC vía la mesa de servicios y apegarse a la normatividad aplicable.

17. El personal de la UTIC que administre la infraestructura de TIC debe evitar el acceso a los respaldos en los medios físicos de información, de personal no autorizado.

18. Las UTIC deben asegurarse de implementar bitácoras de seguridad en las que queden registrados todos

los eventos realizados por cuentas con permisos especiales, al menos: las de administrador, visitante, raíz y de sistema.

19. La UTIC deberá implementar un mecanismo de seguridad para que la bitácora electrónica de auditoría sólo pueda ser consultada por la cuenta de administración del responsable de seguridad del elemento de TIC considerado.

20. La UTIC debe definir e instrumentar un mecanismo de seguridad para evitar intrusiones a la infraestructura de TIC, incluyendo ataques externos vía Internet, extranet e inclusive intranet.

21. La UTIC debe implementar un mecanismo para mantenerse informada de las actualizaciones de seguridad del software utilizado en la dependencia o entidad, de la aparición de nuevos virus informáticos que puedan atacar las soluciones tecnológicas y los equipos de los usuarios de la dependencia o entidad.

22. La UTIC, al identificar la existencia de un virus informático no cubierto por los antivirus institucionales en operación en servidores y en equipos de los usuarios, notificará a la mesa de servicios de manera que, a través de ésta, se difundan las medidas necesarias a los usuarios y éstos se protejan hasta que la UTIC corrija la intrusión del virus y lo elimine.

23. La UTIC deberá instrumentar mecanismos de administración de los equipos de proceso y de comunicaciones, que incluyan revisiones periódicas de las bitácoras de los elementos de la infraestructura de TIC, para identificar si se han presentado intentos de ataques o de explotación de vulnerabilidades.

24. El área de la UTIC deberá habilitar el registro de los incidentes de seguridad relacionados con los accesos a las soluciones tecnológicas y a las actividades realizadas por los usuarios.

A.11 Control de acceso

1. El personal de la UTIC que administre la infraestructura de TIC debe controlar el acceso presencial y remoto a los componentes de cada uno de los elementos de la infraestructura de TIC de la dependencia o entidad.

2. Las UTIC deberán implantar mecanismos de seguridad para acceder a los datos almacenados, que respeten los principios de identidad, responsabilidad y rastreabilidad de los usuarios que los acceden, en función del nivel de exposición y revelación de los mismos.

3. Las UTIC deberán asegurar que las capacidades de los usuarios para acceder a datos están limitadas de acuerdo al perfil que corresponda a sus funciones, previa definición de las UR propietarias de los datos y de las soluciones tecnológicas que hacen uso de ellos.

4. Las UTIC son las encargadas de implementar los mecanismos de seguridad necesarios para la asignación de los permisos de acceso a los usuarios, determinados por las UR responsables de la información.

5. El personal de la UTIC que administre la seguridad de la infraestructura de TIC debe instrumentar el registro de usuarios y la administración de la seguridad de las soluciones tecnológicas de información que son accedidos en forma local y/o remota a través de la red de comunicaciones.

6. El personal de la UTIC que administre la seguridad de la infraestructura de TIC debe instrumentar

mecanismos para que se efectúe la personalización de las cuentas para las actividades de administración de servidores, bases de datos, servicios o sistemas institucionales, así como para el monitoreo de las actividades realizadas por los usuarios.

7. La UTIC deberá instrumentar un mecanismo de seguridad para que, desde su creación, todo usuario tenga definido el ambiente de trabajo acorde a sus funciones; éste no deberá poder ser modificado por el usuario, sino a través de una solicitud a la mesa de servicios.

8. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas deberá asegurar que un solo responsable asigne cuentas de usuario para cualquiera de los servicios y/o sistemas que operan dentro de la dependencia o entidad.

9. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas indicará a los usuarios las características de las contraseñas.

10. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas deberá identificar y autenticar claramente al usuario antes de asignarle una cuenta.

11. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas deberá eliminar cualquier cuenta de usuario que haya cambiado de situación laboral o no labore más en la dependencia o entidad.

12. Las contraseñas no deben ser mostradas en pantalla mientras son tecleadas, ni deben viajar por la red sin ser cifradas.

13. El área de la UTIC designada responsable de la asignación de cuentas de usuario y contraseñas deberá facilitar a los usuarios del correo electrónico, el cambio de contraseña cuando éstos lo estimen conveniente, o de acuerdo en lo establecido en el lineamiento de cambio de contraseña por caducidad

14. Los usuarios deben verificar que su equipo de cómputo tenga configurado el protector de pantalla con contraseña, con la finalidad de evitar el acceso no autorizado a su información en caso de retiro temporal.

15. Los usuarios están obligados a considerar que las cuentas y contraseñas asignadas son personales e intransferibles. Las consecuencias jurídicas y/o administrativas de los actos ejecutados con las mismas son responsabilidad exclusiva del usuario dueño de la cuenta.

16. Los usuarios deben evitar la repetición de contraseñas al efectuar los cambios periódicos de las mismas.

17. Los usuarios deben cambiar su contraseña en caso de sospechar que alguien más la conoce.

18. Los usuarios deben evitar exponer o difundir su contraseña independientemente del medio en el cual sea almacenada.

19. En caso de utilizar hardware de seguridad, tales como generadores de contraseñas o tarjeta inteligente, los usuarios deben traerlos siempre consigo.

20. La UTIC facultará personal técnico para asegurar que todos los equipos de cómputo de escritorio y portátiles que se puedan conectar a la red institucional de la dependencia o entidad cumplan con los siguientes controles de acceso: nombre de equipo que identifique al responsable del equipo y su ubicación;

integración a un dominio; tener instalado el software de antivirus institucional; contar con la última versión y parche del sistema operativo liberado por el proveedor.

21. La UTIC deberá implementar un mecanismo de seguridad en todos los elementos de comunicaciones para que todos los intentos de conexión hacia la infraestructura de TIC que soporta las aplicaciones o servicios institucionales pasen a través de un ”cortafuego” (conocido comúnmente por su traducción en inglés: firewall).

22. La UTIC deberá implementar in situ los mecanismos de seguridad necesarios para el área de producción, y en caso de accesos remotos, deberá instrumentar el uso de software de cifrado de canal.

23. La UTIC deberá implementar un mecanismo de control para proveer el servicio de acceso remoto a la red institucional, a las soluciones tecnológicas, a los servicios de red y colaboración, así como a la información. El acceso será otorgado únicamente a los funcionarios y a los proveedores que lo requieran.

24. La UTIC deberá definir e implementar las herramientas de detección de intrusos y protección a vulnerabilidad alineadas a la infraestructura de TIC, sistemas de información, necesidades de servicios de red y colaboración de la dependencia o entidad.

25. El personal de la UTIC que administre la seguridad de la infraestructura de TIC debe limitar el acceso a los servidores, a sus sistemas operativos, a las soluciones tecnológicas institucionales y a las bases de datos, mediante la identificación del usuario, a través de su cuenta única y contraseña; la UTIC deberá llevar un control de perfil y privilegios de acceso por usuario.

26. La UTIC deberá implementar en las soluciones tecnológicas y servicios a los usuarios, mensajes de ingreso en los cuales se les advierta que: el sistema y/o servicio sólo podrá ser utilizado por personal autorizado, que las actividades realizadas son monitoreadas y rastreables y que cualquier intento de ingreso no autorizado será sancionado.

27. El área de la UTIC responsable de la asignación de cuentas de usuario y contraseñas o en su defecto, las soluciones tecnológicas y aplicaciones, deberán bloquear el acceso a toda cuenta de usuario después de 3 intentos consecutivos fallidos de acceso a las soluciones tecnológicas o red.

28. El área de la UTIC responsable de la asignación de cuentas de usuario y contraseñas o en su defecto, las soluciones tecnológicas y aplicaciones designadas como sensibles o críticas, deberán restringir el número de sesiones por usuario.

29. El área de la UTIC responsable de la asignación de cuentas de usuario y contraseñas, o en su defecto las soluciones tecnológicas y aplicaciones designadas como sensibles o críticas, deberán bloquear cualquier cuenta de usuario que no se haya firmado en el sistema o la red después de 30 días.

A.12 Adquisición, desarrollo y mantenimiento de información

1. La UTIC deberá asegurar que la información institucional que se transmita a través de las redes internas o externas se encuentre cifrada, con independencia de la clasificación confidencial o reservada a la que se encuentre sujeta. Para el caso del almacenamiento de los datos de acuerdo a la clasificación de la información, las definiciones del Grupo de seguridad del SGSI y de los requerimientos que los usuarios definan para sus sistemas o servicios, la información será encriptada.

2. La UTIC deberá implementar un mecanismo de control para que todo el personal responsable o poseedor de manuales, procedimientos, guías e instructivos de operación (en medio electrónico o papel) de los equipos de cómputo, telecomunicaciones y sistemas, controle y reporte el acceso y uso de los mismos, bajo su estricta responsabilidad.

A.13 Gestión de incidentes en la seguridad de la información.

1. Los usuarios que presencien o sospechen actos citados en la disposición anterior deberán notificarlo por escrito a su inmediato superior y al responsable del área de seguridad de la información.

2. El siniestro, extravío o robo de equipo de cómputo y/o periféricos deben ser reportados de forma inmediata por el usuario afectado (aquel que tiene bajo su resguardo el equipo siniestrado) al área administrativa correspondiente, para que se realicen las gestiones pertinentes

A.15 Cumplimiento

1. Los datos clasificados como confidenciales o reservados deberán tener fechas programadas de eliminación y deberá destruirse la identificación del medio y cualquier marca de uso, en estricto apego a la normatividad vigente en la materia y asegurando conservar la evidencia correspondiente del apego a la regla.

2. La información confidencial o reservada no necesaria deberá ser destruida, los listados deberán ser triturados y los desechos empacados antes de deshacerse de ellos, en estricto apego a la normatividad vigente en la materia y asegurando conservar la evidencia correspondiente del apego a la regla.

3. En caso de inobservancia y, a fin de garantizar la integridad, confiabilidad y disponibilidad de la información de las Instituciones, el personal responsable de la seguridad de los recursos de TIC tendrá la obligación de suspender de manera inmediata los servicios de TIC al o los usuarios que hubieren infringido alguna de las disposiciones del presente manual.

4. La UTIC deberá asegurarse de que cualquier intento para obtener acceso no autorizado a la infraestructura, a los servicios o a los datos, la revelación no autorizada de información, el procesamiento, almacenamiento o transmisión de datos, los cambios a las características de los activos de TIC sin autorización, o cualquier otra actividad en materia de TIC, que afecte a los intereses de la dependencia o entidad, sean informados a las instancias facultadas, para promover las sanciones aplicables de acuerdo a la reglamentación y la legislación vigente aplicable.