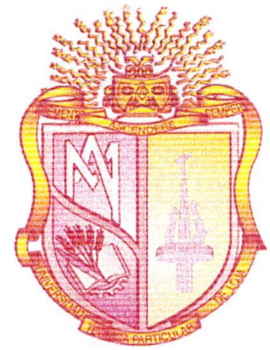
UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA



UNIVERSIDAD TÉCNICA
PARTICULAR DE LOJA
La Universidad Católica de Loja

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA PARA BASES DE DATOS EN PYMES

EDWIN PATRICIO MÁRQUEZ CADENA

Junio de 2007

Manual de Políticas y procedimientos para bases de datos en PYMES

Autor: Edwin Patricio Márquez Cadena

Junio de 2007

Manual de Políticas Informáticas para bases de datos en PYMES

Autor: Edwin Patricio Márquez Cadena

Junio de 2007

Índice

Esquema de contenidos

Introducción

Luego de haber realizado el respectivo análisis de riesgos y la proposición de controles en las matrices de riesgos de las dos empresas estudiadas, ello permite que sean identificados los puntos críticos en las áreas de gestión de los distintos SGBD utilizados por las organizaciones, con el objetivo de implementar políticas de seguridad en un ambiente tecnológico y humano.

El siguiente paso es delinear estas políticas y establecer las normas que deben ser seguidas por todos los involucrados en la operación y el uso de las bases de datos, su información y los diversos activos de la organización.

Estas políticas se elaboran tomando en cuenta el entorno de trabajo y las áreas de gestión que conforman las bases de datos de las organizaciones, los criterios a aplicar en el ámbito de la seguridad de la información están de acuerdo con las actuales prácticas adoptadas en la mayoría de las organizaciones a nivel mundial y tomando como base estándares de la Norma IRAM-ISO IEC 17799.

La importancia de aplicar estas políticas radica en que al ponerlas en práctica, el personal encargado del manejo y la operación de la(s) base(s) de datos de las empresas tengan presente y pongan en práctica lineamientos que le ayuden a realizar una gestión diaria eficiente, eficaz y sobretodo manteniendo las observancias que sobre seguridad informática utiliza su empresa.

Objetivos

- Emplear los conceptos básicos de seguridad aplicables a la generación de políticas de seguridad para las Bases de Datos de las PYMES, por su intermedio permitir que éstas abarquen todos los aspectos necesarios de la seguridad y lograr una exitosa implantación de las mismas.

- Identificar los controles de seguridad propuestos en las matrices de análisis de riesgos, los mismos que deben lograr el equilibrio entre el nivel de seguridad y el nivel de comodidad, además ellos deben estar reflejados en estas políticas de seguridad.

- Elaborar y entregar el documento de proyecto de tesis para que sirva en las empresas para capacitar y dar a conocer a los usuarios de bases de datos temas sobre seguridad informática, políticas de seguridad informática, para lograr instaurarlas en la cultura organizacional de las empresas.

1. Seguridad del personal

Objetivo.- Mitigar los riesgos de fraude, uso inadecuado de las instalaciones, fraude y robo en la empresa.

1.1. Seguridad en las responsabilidades de los puestos de trabajo

- Las funciones y responsabilidades en materia de seguridad deben ser de un alto grado de formalización y documentadas de una manera organizada. Éstas contienen; responsabilidades generales por implementación, mantenimiento de la política de seguridad, además deben incluir responsabilidades específicas en la protección de activos, por la ejecución de procesos o acciones de seguridad específicas.

1.2. Términos y condiciones de empleo

- En las condiciones y términos de empleo, se deben establecer las responsabilidades del empleado por la seguridad de la información. Estas responsabilidades deben mantenerse hasta el fin la relación laboral. Se deben definir las acciones administrativas o legales que se ejecutarán si el empleado no cumple con los requerimientos de seguridad.

- Los derechos legales y responsabilidades del empleado; en relación con los derechos de propiedad intelectual, deben ser clarificados e incluidos en los términos y condiciones del contrato de empleo.

- Los términos y condiciones de empleo deben establecer la responsabilidad por la clasificación y administración de los datos del empleador. Cuando corresponda, los términos y condiciones de empleo deben establecer que estas responsabilidades se extienden más allá de los límites de la sede de la organización y del horario normal de trabajo.

1.3. Acuerdos de confidencialidad

- Los acuerdos de confidencialidad (de no divulgación de la información), deben ser parte fundamental en la elaboración de cada contrato con el o los aspirantes a trabajar en la organización siendo parte de sus términos y condiciones iniciales de empleo.

- El personal ocasional y los usuarios externos aún no contemplados en un contrato formalizado (que contenga el acuerdo de confidencialidad) deberán firmar el mencionado acuerdo antes de que se les conceda acceso a los servicios de procesamiento de información.

2. Capacitación del usuario

Objetivo: Avalar que los usuarios están al corriente de los riesgos y amenazas que podrían afectar a la información contenida en las bases de datos de la organización, así como los ámbitos de seguridad y deben estar capacitados para respaldar la política de seguridad informática de la organización en el transcurso de sus tareas normales.

- Los usuarios deben ser capacitados en el correcto uso de la información en concordancia con los procedimientos de seguridad, las instalaciones de procesamiento de la misma, a fin de reducir imprevistos riesgos de seguridad.

- Todos los usuarios de bases de datos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de seguridad, políticas y procedimientos de la organización. Entre ellos; requerimientos de seguridad, las responsabilidades legales y controles del negocio, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, por ejemplo; el procedimiento de entrada al sistema ("log-on") y el uso de la(s) bases de datos, antes de que se les otorgue acceso a la información o a los servicios de las mismas.

2.1. Formación y capacitación en materia de seguridad de la información a los empleados de la organización

- Los usuarios de las bases de datos deben ser capacitados en procedimientos de seguridad, el adecuado uso de las instalaciones de procesamiento de información, a fin de mitigar eventuales riesgos de seguridad.

- Se debe capacitar al personal de una manera adecuada y mantener actualizaciones periódicas en materia de políticas y procedimientos de seguridad informática para bases de datos en la organización. Y, cuando sea acertado también a los usuarios externos con alcance a los requerimientos de seguridad, controles del negocio y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, por ejemplo; el procedimiento de entrada a la base de datos ("log-on") y el uso de paquetes de software, antes de que se les otorgue acceso a la información o a los servicios.

3. Respuesta a incidentes y anomalías en materia de seguridad

Objetivo: Mitigar el daño producido por anomalías e incidentes en materia de seguridad informática, y monitorearlos para aprender de los mismos.

- Se debe concienciar a todos los empleados y contratistas acerca de los procedimientos de comunicación de los diferentes tipos de incidentes (amenazas, violaciones, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los SGDB y en los activos de la organización. Se debe requerir que los mismos comuniquen cualquier incidente advertido o supuesto al personal encargado o a sus superiores tan pronto como sea posible.

- Los incidentes que puedan afectar a la seguridad de las bases de datos deben ser comunicados mediante canales gerenciales adecuados tan pronto como sea posible.

- Para lograr abordar debidamente los incidentes ocurridos podría ser necesario recolectar evidencia en los SGDB tan pronto como sea posible una vez ocurrido el hecho.

- Se debe establecer un proceso disciplinario formal en la organización, el mismo que se ocupe de los empleados que cometan violaciones en contra de la seguridad de la(s) base(s) de datos de la organización.

3.1. Comunicación de incidentes relativos a la seguridad

- Se debe establecer un procedimiento formal de comunicación, conjuntamente con un procedimiento de respuesta a incidentes, que instaure la acción que se ha de ejecutar al recibirse un informe sobre incidentes ocurridos en las bases de datos y aplicaciones de la organización.

- Todos los empleados de la organización deben estar al corriente del procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos a través de los canales gerenciales en forma ágil y oportuna.

- Deben efectuarse adecuados procesos de "feedback" para garantizar que las personas que comunican los incidentes sean notificadas de los resultados una vez tratados y resueltos dichos incidentes.

- Los incidentes ocurridos pueden utilizarse en la capacitación a fin de crear conciencia de seguridad informática en el usuario como ejemplo de lo que puede ocurrir, de cómo responder a dichos incidentes y de cómo evitarlos en el futuro.

3.2. Comunicación de debilidades en materia de seguridad

- Los usuarios de las bases de datos y servicios de información deben advertir, registrar y comunicar las debilidades, amenazas supuestas u observadas en materia de seguridad, con relación a los sistemas o servicios. Estos asuntos deberán comunicar a su respectiva jefatura, gerencia, o directamente a su proveedor de servicios, tan pronto como sea posible.

3.3. Proceso disciplinario

- Se debe implantar sanciones y elementos disuasivos en relación a la violación de normas de seguridad informática mediante un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización.

- Se debe formalizar un proceso disciplinario para los empleados que incurran en la violación de procedimientos y políticas de seguridad de la información contenida en las bases de datos de la organización. Este proceso debe ser justo e imparcial hacia el empleado sospechoso de haber ejecutado violaciones en contra de la seguridad.

4. Seguridad física y ambiental

4.1. Áreas seguras

Objetivo: Impedir accesos no autorizados, daños, obstrucción a las sedes e información contenida en las bases de datos de la organización.

- Las instalaciones de procesamiento de información crítica o sensible de la organización deben estar ubicadas en áreas protegidas, resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados.

- Las áreas críticas deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones.

- La protección provista debe ser proporcional a los riesgos identificados. Se sugiere la implantación de políticas de pantallas y escritorios limpios para minimizar el riesgo de accesos no autorizados o de daño a papeles, medios de almacenamiento e instalaciones de procesamiento de información.

- Se debe adoptar una política de escritorios limpios para proteger los documentos en papel y dispositivos magnéticos de almacenamiento removibles. Además de una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo, se deben considerar los siguientes lineamientos:

- Los documentos en papel y los medios magnéticos deben ser almacenados en sitios seguros bajo llave cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

- La información respaldada en backup o copias de seguridad de la base de datos, información sensible o crítica de la empresa debe guardarse bajo llave (de preferencia en una caja fuerte ignífuga) cuando no está en uso, especialmente cuando no hay personal en la oficina.

- Las terminales, computadoras personales e impresoras no deben dejarse conectadas cuando están desatendidas; las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso.

- Se deben proteger los puntos de recepción, envío de correo, las máquinas de fax y telex no atendidas.

- La información sensible o confidencial de base de datos y aplicaciones, una vez impresa, debe ser retirada de la impresora inmediatamente.

4.2. Perímetros de seguridad física

Un perímetro de seguridad esta delimitado por ejemplo por una pared, una puerta, oficina de recepción, una puerta de acceso controlado con tarjeta, etc.

Se deben considerar e implementar las siguientes políticas, según corresponda:

- El contorno de seguridad física debe estar claramente definido.

- Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio. El acceso a las distintas áreas y edificios debe estar restringido exclusivamente al personal no autorizado.

- El perímetro del área en la que existan instalaciones de procesamiento de información debe ser físicamente sólido, es decir; no deben existir claros o aberturas en el perímetro o sitios donde pueda producirse fácilmente una irrupción.

- Las paredes externas del área de seguridad deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ejemplo; mediante mecanismos de control, alarmas, vallas, cerraduras, etc.

- Todas las puertas de incendio de un perímetro de seguridad física deben tener alarma y cerrarse automáticamente.

- Las barreras físicas deben extenderse desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo; la ocasionada por incendios e inundaciones.

4.3. Control de acceso físico

- Las visitas a las áreas protegidas deben ser supervisadas o inspeccionadas, la fecha, hora de su ingreso y salida deben ser registradas.

- El acceso a las áreas protegidas sólo se lo debe permitir con propósitos específicos y mediante autorización, se debe instruir al visitante sobre los requerimientos de seguridad y los procedimientos de emergencia.

- Todo el personal de la organización debe exhibir su tarjeta de identidad o alguna otra forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados esto es a cualquier persona que no exhiba una identificación visible.

- El acceso a las instalaciones de procesamiento de información sensible, debe ser controlado y limitado exclusivamente al personal no autorizado.

- Se deben utilizar controles de autenticación, por ejemplo; tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos.

- En el SGDB debe mantenerse una pista protegida que permita auditar todos los accesos.

- Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

4.4. Protección de oficinas, recintos e instalaciones

Un área protegida puede ser una oficina protegida con llave, o diversos perímetros dentro de un contorno de seguridad física, el cual puede estar bloqueado y contener cajas fuertes o gabinetes con cerraduras. Para la selección y el diseño de áreas protegidas se debe advertir la posibilidad de daño producido por inundación, incendio, agitación civil, explosión, desastres naturales o provocados. Igualmente deben tomarse en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad,

también se deben considerar amenazas a la seguridad que representan edificios y zonas aledañas, por ejemplo filtración de agua desde otras áreas.

- Las instalaciones claves o áreas críticas deben ubicarse en lugares a los cuales no pueda acceder el público.

- Los cuartos de servidores de bases de datos y las instalaciones de procesamiento de información administradas por la organización deben estar físicamente separadas de aquellas administradas por terceros.

- Los edificios y áreas críticas deben ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, que identifiquen la presencia de actividades de procesamiento de información.

- El equipamiento de soporte y hardware, por ejemplo; impresoras, fotocopiadoras, máquinas de fax, deben estar adecuadamente ubicados dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

- El equipamiento de sistemas de soporte UPC (Usage Parameter Control) de reposición de información perdida ("fallback") y los medios informáticos de resguardo deben estar ubicados a una distancia prudencial para evitar daños producidos por eventuales desastres en el sitio principal.

- Los centros de cómputo y salas de comunicaciones deben ser protegidos y mantener alarmas activadas en todo momento, también se deben proteger las áreas vacías.

- Los combustibles o materiales peligrosos deben ser almacenados en sitios seguros y a una distancia prudencial del área protegida.

- Los listados telefónicos internos y sus extensiones que identifiquen las ubicaciones de las instalaciones de procesamiento de información sensible no deben ser fácilmente accesibles al público.

5. Seguridad frente al acceso físico por parte de terceros

Objetivo: Conservar la seguridad de las instalaciones de procesamiento de información y de los recursos de la organización a los que acceden terceras partes.

- El acceso físico a las instalaciones de procesamiento de información de la organización por parte de terceros debe ser controlado.
- Los controles deben ser acordados y definidos en un contrato formal con la tercera parte.
- Dada la necesidad de la organización para permitir dicho acceso, debe realizarse una evaluación de riesgos para determinar posibles incidentes en la seguridad y los requerimientos de control.
- El acceso de terceros también puede involucrar otros participantes. Los contratos que confieren acceso a terceros deben incluir un permiso para la designación de otros participantes capacitados y las condiciones para su acceso. Este estándar puede utilizarse como base para tales contratos y cuando se considere la tercerización del procesamiento de información.

5.1. Contratistas in situ

Las terceras partes que sean aceptadas en el sitio por un lapso de tiempo establecido según estipulación, también pueden ocasionar debilidades en materia de seguridad. Entre los ejemplos de terceras partes in situ se listan los siguientes:

a) Consultores

b) Limpieza, "catering", guardianía de seguridad y otros servicios de soporte tercerizados

c) Personal de mantenimiento / soporte de hardware / soporte de software

d) Pasantías de estudiantes y otras designaciones contingentes de corto plazo

Es primordial establecer qué controles son precisos para gestionar el acceso de terceras partes a la infraestructura de procesamiento de información, todos los requerimientos de seguridad que reflejan los controles internos o del acceso de terceros, estarán presentes en los contratos celebrados con los mismos.

5.2. Requerimientos de seguridad en contratos con terceros

- No se debe otorgar a terceros acceso a la información ni a las instalaciones de procesamiento de la misma mientras no se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones para la conexión o para el acceso.
- Las instrucciones que observan el acceso de terceros a las instalaciones de procesamiento de información de la organización deben estar instituidas en un contrato formal que contenga todos los requerimientos de seguridad, o haga

referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y estándares (normas) de seguridad de la organización.

- El contrato debe garantizar que no surjan malentendidos entre la organización y el proveedor. Las organizaciones deben estar satisfechas con las garantías de su proveedor.

- Se deben considerar las siguientes cláusulas para su inclusión en el contrato:

  - La defensa de activos, incluyendo:

    1) Procedimientos para estipular si se han comprometido los activos, por ejemplo; debido a pérdida o modificación de datos

    2) Procedimientos de resguardo de los activos más importantes de la organización, sobretodo; información y software

    3) Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato, o en un momento convenido durante la vigencia del mismo

    4) Restricciones a la copia y divulgación de información

    5) Integridad y disponibilidad

  - Un diseño de los servicios de los cuales podrá disponerse

  - La política general de seguridad de la información

  - Disposición que contemple la transferencia de personal cuando corresponda

  - El nivel de servicio al que se aspira y los niveles de servicio que se consideran inaceptables.

  - Las pertinentes obligaciones de las partes con relación al acuerdo

  - Compromisos con respecto a asuntos legales, por ejemplo, si hubiese una necesidad específica de confidencialidad de la información, podrían implementarse acuerdos de no-divulgación.

  - Derechos de propiedad intelectual y asignación de derecho de propiedad intelectual, y protección de trabajos realizados en colaboración

  - Acuerdos de control de accesos que contemplen:

    1) Los métodos de acceso permitidos, y el control y uso de identificadores únicos como ID´s y contraseñas de usuarios

    2) Un proceso de autorización de acceso y privilegios de usuarios

    3) Un requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

- El derecho a monitorear, y revocar (impedir), la actividad del usuario

- El derecho a auditar responsabilidades contractuales o a contratar a un tercero para la realización de dichas auditoríass
- La definición de criterios de desempeño comprobables, y el monitoreo y presentación de informes respecto de los mismos
- La instauración de un proceso paulatino para la resolución de problemas; deben contemplarse, si corresponde, disposiciones con relación a situaciones de contingencia
- Responsabilidades relativas a la instalación y el mantenimiento de hardware y software
- Una clara estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos
- Un proceso claro y detallado de administración de cambios
- Los controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos
- Los métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad
- Los controles que garanticen la protección contra software malicioso
- Las instrucciones con respecto a elaboración y presentación de informes, investigación e institución de incidentes y violaciones relativos a la seguridad
- La relación entre proveedores y subcontratistas.

5.3. Desarrollo de tareas en áreas protegidas

- Se debe evitar el trabajo no controlado en las áreas protegidas tanto por razones de seguridad así como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.
- Las áreas protegidas evacuadas deben ser físicamente bloqueadas y periódicamente inspeccionadas.
- El personal del servicio de soporte externo debe tener acceso limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso debe ser otorgado solamente cuando sea necesario, debe ser autorizado y monitoreado. Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- No debe permitirse el ingreso de equipos fotográficos, dispositivos de almacenamiento USB para vídeo, audio u otro tipo de equipamiento que registre información a las áreas críticas de la organización a menos que su ingreso se autorice expresamente.

6. Seguridad de los equipos

Objetivo: Evitar las pérdidas, daños o exposiciones al riesgo de los activos e interrupción de las actividades de la empresa.

- Los equipos deben estar físicamente protegidos de los peligros del entorno y de las amenazas a la seguridad.

- Es precisa la protección de los equipos (incluyendo los que se utilizan en forma externa) para minimizar los riesgos de acceso no autorizado a los datos y para prevenir pérdidas o daños.

- Se debe tener en cuenta la ubicación y disposición equipamiento, puede que se requieran controles especiales para advertir peligros ó accesos no autorizados, para salvaguardar instalaciones de soporte, como la instalaciones de cableado y provisión de energía eléctrica.

6.1. Ubicación y protección de los equipos

Los equipos deben ser ubicados y protegidos de manera que se mitiguen los riesgos originados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.

Se debe considerar los siguientes puntos:

- Los equipos que requieren protección especial deben ser aislados para reducir el nivel general de protección requerida.

- El equipamiento debe ser ubicado en un sitio que permita minimizar el acceso innecesario a las áreas de trabajo.

- Se deben adoptar controles especiales para minimizar el riesgo de amenazas potenciales, por ejemplo; incendio, robo, explosivos, humo, agua (o falta de provisión), vibraciones, polvo, efectos químicos, radiación electromagnética, interrupción en el suministro de energía eléctrica.

- El sitio de procesamiento y almacenamiento de información, que maneja datos sensibles, debe ubicarse en un lugar que permita minimizar el riesgo de falta de supervisión de las mismas durante su uso.

- Se debe utilizar protección especial para equipos, ejemplo; membranas de teclado, para los equipos ubicados en ambientes industriales, etc.

- Se debe considerar la ocurrencia de un eventual desastre en zonas próximas a la sede de la organización, por ejemplo; un incendio en un edificio cercano, la filtración de agua desde el cielo raso o en pisos por debajo del nivel del suelo o una explosión en la calle.

- Se debe, prohibir, establecer normas y sanciones respecto a comer, beber y fumar cerca de las instalaciones de procesamiento de información.

- Se deben monitorear las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de los servidores de bases de datos y a las instalaciones de procesamiento de la información.

6.2. Suministros de energía

- El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. Se debe contar con un adecuado suministro de energía que esté de acuerdo con las especificaciones del fabricante o proveedor de los equipos.

Entre las alternativas para asegurar la continuidad del suministro de energía podemos enumerar las siguientes:

- Múltiples entradas de suministro para evitar un único punto de falla en el suministro de energía
- Suministro de energía ininterrumpible (UPS)
- Generador de respaldos de SGBD.
- Se recomienda una UPS para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la organización. Los planes de contingencia deben contemplar las acciones que han de emprenderse ante una falla de la UPS.
- Los equipos de UPS deben inspeccionarse periódicamente para asegurar que tienen la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor.
- Se debe tener en cuenta el empleo de un generador de respaldo si el procesamiento ha de continuar en caso de una falla prolongada en el suministro de energía. De instalarse, los generadores deben ser probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor. Se debe disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado.
- Los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.
- Para áreas críticas y centros de procesamiento de datos, se debe proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.
- Se debe implementar protección contra rayos en todos los edificios, así como adaptación filtros de protección contra rayos en todas las líneas de comunicaciones externas.

7. Gestión de comunicaciones y operaciones

7.1. Procedimientos y responsabilidades operativas

Objetivo: Garantizar el seguro y correcto funcionamiento de las instalaciones de procesamiento de la información.

- Se deben establecer las responsabilidades, procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Esto incluye el desarrollo de instrucciones operativas y procedimientos apropiados de respuesta a incidentes.

- Se debe implementar la separación de funciones cuando corresponda, a fin de reducir el riesgo del uso negligente o mal uso deliberado del SGDB.

7.2. Documentación de los procedimientos operativos

- Se deben formalizar y documentar los procedimientos operativos para cada área de gestión de las bases de datos. Los cambios que se realicen a los procedimientos operativos deben ser autorizados por el nivel gerencial.

- Las instrucciones y procedimientos que se deben especificar para la ejecución detallada de cada tarea, debe incluir:

- Manejo y procesamiento de la información contenida en las bases de datos

- Las interdependencias con otros sistemas, tiempos de inicio de primeras tareas y tiempos de terminación de últimas tareas, así como requerimientos de programación ("schedulling").

- Instrucciones para el manejo de condiciones excepcionales y errores que podrían surgir durante el cumplimiento de tareas, además se debe tener en cuenta las restricciones en el uso de utilitarios del sistema.

- Personal de soporte a ser contactado en caso de dificultades operativas o técnicas imprevistas.

- Reinicio del sistema y procedimientos de recuperación en caso de producirse fallos en el mismo, así como la recuperación del SGDB.

- Instrucciones especiales para el manejo de salidas ("outputs"), como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas de tareas fallidas.

- Documentación sobre procedimientos de actividades de mantenimiento del sistema, relacionadas con los servicios de procesamiento de información y comunicaciones, documentación de procedimientos de inicio y cierre, mantenimiento de equipos, resguardo, salas de cómputo, administración, resguardo y seguridad del manejo de correo.

7.3. Control de cambios en las operaciones

- Se deben vigilar las instalaciones de procesamiento de datos y los cambios que se realicen en los sistemas de información. Un control inadecuado de estos cambios es una causa común de las fallas de seguridad y de los sistemas.

- Los programas operativos deben ser sometidos a un control estricto de cambios. Cuando se realizan cambios en los programas, se debe llevar un registro de auditoría que contenga toda la información principal.

- Se debe garantizar que los controles de cambios logren implementar; responsabilidades y procedimientos gerenciales formales que garanticen un control satisfactorio de todos los cambios en el equipamiento, el software o los procedimientos.

- "Los cambios en el ambiente operativo pueden tener impacto en las aplicaciones. Siempre que sea factible, los procedimientos de control de cambios en las operaciones y aplicaciones deben estar integrados. Se debe considerar:

- Identificación y registro de cambios significativos

- Procedimiento de aprobación formal de los cambios propuestos

- Evaluación del posible impacto de dichos cambios

- Comunicación de detalles de cambios a todas las personas que sea pertinente

- Procedimientos que identifican las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos." [1]

- Los cambios que se realicen en los SGDB; en sus estructuras de datos, así como al realizar migraciones de datos deben estar basados en controles, mientras se realicen estos cambios, las bases de datos no deben estar abiertas y/o arrancadas.

7.4. Procedimientos de manejo de incidentes

- Se deben establecer procedimientos y responsabilidades para el manejo de incidentes con la finalidad de garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

Se debe considerar:

a) Se deben establecer procedimientos que contemplen todos los tipos probables de incidentes relativos a seguridad, incluyendo:

   1) Fallas en los SGDB y pérdida del servicio

   2) Negación del servicio

   3) Violaciones de la confidencialidad

   4) Errores ocasionados por datos comerciales incompletos o inexactos

b) Los planes de contingencia deben ser diseñados para recuperar sistemas y servicios de una forma inmediata y ágil tan pronto como sea posible, además en sus procedimientos se deben contemplar:

   1) Identificación y análisis de la(s) causa(s) del incidente.

   2) Evitar la repetición de incidentes mediante la planificación e implementación de soluciones.

   3) Recolección de pistas de auditoría y evidencia similar.

   4) Comunicación con el personal afectado e involucrado con la recuperación, del incidente.

   5) Comunicar de las acciones a tomar a la autoridad pertinente.

c) Se deben reunir, resguardar pistas de auditoría y evidencia similar, según atañe para:

   1) Uso como evidencia en relación con una probable violación de contrato, de requisito normativo, o en el caso de un proceso judicial civil o criminal, por ejemplo por aplicación de legislación sobre fraude informático o protección de datos.

   2) Uso de evidencia para el análisis de problemas internos.

   3) Negociación de indemnizaciones por parte de los proveedores de software y de otros servicios;

d) Se deben instaurar controles precisos y formales de las acciones de recuperación respecto de las infracciones de la seguridad y de corrección de fallas del sistema. Los procedimientos deben garantizar que:

   1) Sólo se otorgue acceso a las bases de datos, a los datos o a la información existente al personal claramente identificado y autorizado.

   2) Todas las acciones de emergencia realizadas deben ser documentadas en forma clara y detallada, además deben ser comunicadas a la gerencia y ser revisadas en forma periódica.

   3) Los plazos para constatar la integridad de los controles y sistemas de la empresa deben establecerse como mínimos.

7.5. Separación de funciones

- Se debe minimizar el riesgo por mal uso; sea accidental o deliberado del SGBD mediante la separación de funciones.

- A fin de reducir las oportunidades de modificación no autorizada o mal uso de la información contenida en las bases de datos u otros servicios, se debe considerar la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad.

- Cuando sea difícil llevar a cabo la separación de funciones, se deben llevar a cabo tareas de; supervisión gerencial, el monitoreo de las actividades, pistas de auditoría.

- Los SGBD y las aplicaciones deben incorporar procesos que faciliten la realización de auditorías, por ejemplo; el registro de accesos exitosos y fallidos al SGBD, registro de transacciones, etc.

- El proceso de respaldo debe ser realizado de una forma adecuada y segura, éste proceso debe garantizar la correcta restauración de los datos para cuando se los requiera.

- Todo SGDB que pretenda ser seguro debe mantener registros de auditoría adecuados al entorno, no basta con controlar quien entra, a dónde accede, sino que se debe registrar quién, cuándo, desde dónde, a que accede, y cómo accede para en base a ello poder obtener información de auditoría. La auditoría no es in sistema preventivo, sino que sirve para detectar comportamientos no adecuados y es muy útil para la recuperación de sistemas. En los SGDB da información de lo que ocurrió, ayuda en gran medida a saber cómo devolver el sistema a la normalidad, así como para implantar en el futuro medidas para evitar que sigan ocurriendo deficiencias en la seguridad.

- En una base de datos Oracle se debe auditar todas las acciones que tienen lugar en ella. Los registros de auditoría pueden escribirse tanto en la tabla SYS.AUD$ como en la pista de auditoría de sistema operativo. La capacidad de utilizar las pistas de auditoría de sistema operativo depende de él mismo.

- En los SGDB se deben auditar tres tipos distintos de acciones:

- Intentos de inicio de sesión

- Accesos a objetos y

- Acciones de la base de datos

- Es recomendable que la gestión de auditoría informática permanezca independiente de otras funciones.

- Deben tomarse previsiones para que ninguna persona pueda perpetrar un fraude en áreas de responsabilidad única sin ser detectada. El inicio de un evento debe estar separado de su autorización.

Se deben considerar:

a) Si existe peligro de confabulación, los controles deben ser diseñados de manera tal que dos o más personas deban trabajar conjuntamente, reduciendo de ese modo la posibilidad de conspiración.

b) Es importante separar actividades que confabulen para defraudar, por ejemplo; efectuar una orden de compra y verificar que la mercadería fue recibida.

7.6. Separación entre instalaciones de desarrollo e instalaciones operativas

- Se deben definir y documentar de una manera muy formal las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.
- De manera deseable se deben separar las instalaciones de desarrollo, prueba y operaciones para así lograr también la separación de los roles involucrados.
- Las actividades de desarrollo y prueba pueden ocasionar problemas graves, como la modificación no deseada de archivos o sistemas, o la rectificación no deseada de fallas de sistemas.
- Se debe considerar el nivel de separación que resulta necesario entre los ambientes operativos, de prueba y de desarrollo, a fin de prevenir problemas operativos.
- Se debe implementar una separación similar entre las funciones de desarrollo y prueba. Si existe la necesidad de mantener un ambiente conocido y estable en el cual puedan llevarse a cabo pruebas demostrativas y evitar accesos no autorizados por parte del personal de desarrollo.
- Se debe evitar el acceso a las áreas de desarrollo o áreas operativas ya que si el personal de desarrollo y prueba tiene acceso al sistema que esta operativo y o a su información, éste podría introducir líneas de código no autorizados o no probados, o alterar los datos de las operaciones.
- Las actividades de desarrollo y pruebas pueden producir cambios no planificados en el software y la información si los sistemas comparten el mismo ambiente informático.
- La separación entre las instalaciones de desarrollo, pruebas y operaciones es deseable, a fin de reducir el riesgo de cambios accidentales o accesos no autorizados al software operativo y a los datos del negocio.

Se deben tener en cuenta:

- Es necesario que las actividades de desarrollo y prueba estén separadas.
- De una manera deseable, el software en desarrollo y el software de operaciones deben ejecutarse en diferentes directorios, dominios o diferentes procesadores.
- Es deseable que los editores, compiladores y otros utilitarios del sistema no sean accesibles desde los sistemas que están operativos.
- El personal de desarrollo sólo debe tener acceso a las contraseñas operativas. Estos controles deberán garantizar que estas contraseñas se cambien una vez utilizadas.
- A fin de reducir el riesgo de error, se deben utilizar diferentes procedimientos de conexión ("log-on") para sistemas èn operación y prueba. Se debe alentar a los usuarios a utilizar diferentes contraseñas para estos sistemas, y los menús deben desplegar adecuados mensajes de identificación.

7.7. Administración de instalaciones externas

- Cuando una organización utilizase a un contratista externo para la administración de las instalaciones de procesamiento de información hay que considerar que esto puede dar lugar a potenciales exposiciones al riesgo en materia de seguridad. Estos riesgos deben ser identificados con anticipación, y deben acordarse controles adecuados con el contratista e incluirse en el contrato para orientación con respecto a contratos con ellos u otros terceros que contemplan el acceso a instalaciones de la organización y contratos de tercerización.

Se deben abordar las siguientes cuestiones:

- Obtener la aprobación de los propietarios de aplicaciones comerciales.
- Asignación de responsabilidades específicas y procedimientos para monitorear con eficacia todas las actividades de seguridad pertinentes.
- Identificar las aplicaciones sensibles o críticas que convienen retener en la organización.
- Responsabilidades y procedimientos de comunicación y el manejo de incidentes relativos a la seguridad.
- Implicancias para la continuidad de los planes comerciales.
- Estándares de seguridad a especificar, y el proceso de medición del cumplimiento.

8. Planificación y aprobación de sistemas

Objetivo: Mitigar el riesgo de ocurrencia de fallos en los sistemas.

- Anticipadamente se debe realizar una planificación y preparación para garantizar la disponibilidad de capacidad y recursos adecuados.
- Antes de la aprobación y uso de los nuevos sistemas, se deben documentar y probar los requerimientos operativos.
- A fin de reducir el riesgo de sobrecarga del sistema, deben efectuarse proyecciones para futuros requerimientos de capacidad.
- Cada vez que se cree una base de datos, el DBA o la persona encargada debe asignar el tamaño que ocupará la misma de una manera provisoria.
- Así mismo el DBA debe ser provisorio al asignar el tamaño de las tablas y vigilar el crecimiento descontrolado de la memoria de las bases de datos, debe asegurar que exista el suficiente espacio para almacenar los objetos y la información de los usuarios
- El DBA o la persona encargada debe decidir las cuotas o tamaño de disco a utilizarse por cada base de datos o usuario.
- Para mantener en un alto performance los recursos del equipo servidor y evitar la merma en los recursos, se dará instrucciones claras sobre el respeto a los horarios de obtención de backups y copias de respaldo, los mismos no se los realizará en horas laborables.

9. Gestión de Bases de Datos

La gestión de bases de datos abarca las áreas de administración, seguridad y migración de datos.

9.1. Planificación de la capacidad

- Los administradores de servicios mainframe o administradores bases de datos deben realizar una constante supervisión de los recursos del sistema, incluyendo procesadores, almacenamiento de archivos, almacenamiento principal, almacenamiento secundario, otros medios de salidas ("outputs"), y sistemas de comunicaciones. Ésta supervisión debe establecer las preferencias de uso, concretamente en relación con las bases de datos y/o sistemas de información de la organización.

- Se deben monitorear las demandas de capacidad y realizar proyecciones de sus futuros requerimientos, con el fin de garantizar la disponibilidad del poder de procesamiento y almacenamiento adecuados. Estas proyecciones deben tomar en cuenta los nuevos requerimientos de negocios, sistemas, las tendencias actuales y proyectadas en el procesamiento de la información de la organización.

- Los DBA deben utilizar esta información para identificar y evitar potenciales cuellos de botella que podrían plantear una amenaza a la seguridad del SGDB, sistemas o a los servicios del usuario, y planificar una adecuada acción correctiva.

9.2. Aprobación del sistema

- Se deben instaurar juicios de aprobación para SI nuevos que trabajen o tengan enlaces con las bases de datos de la organización, actualizaciones ("upgrades"), nuevas versiones, y se deben realizar apropiadas pruebas de los sistemas antes de su aprobación.

- Los gerentes deben garantizar que los requerimientos y criterios de aprobación de nuevos sistemas sean claramente definidos, acordados, documentados y probados.

Se debe considerar:

- Requerimientos, desempeño y capacidad de las computadoras.

- Procedimientos de reinicio, recuperación ante errores y elaboración de planes de contingencia.

- Preparación y prueba continua de procedimientos operativos de rutina según estándares definidos.

- Acordar un conjunto de controles de seguridad a implementar.

- Establecer procedimientos manuales eficaces.

- Certificar mediante evidencias que la instalación del nuevo sistema no afectará negativamente los sistemas en funcionamiento, primordialmente en las fases pico del procesamiento de datos.

- Asegurar mediante evidencias que se ha tomado en cuenta el efecto que tiene el nuevo sistema en la seguridad integral de la organización.

- Se debe dar al personal entrenamiento para la operación y uso de nuevos sistemas a implantarse.

- Para la capacidad de recuperación de las bases de las bases de datos se las debe llevar a cabo mediante las utilidades; export (exportar) e import (importar), los mismos que forman parte de la mayoría de los planes de copias de seguridad y recuperación para bases de datos pequeñas y para DB's en desarrollo.

- La capacidad de recuperación de los SGBD debe ser probada de forma periódica y ésta debe garantizar su óptima recuperación y la continuidad del negocio de las organizaciones. Con la utilidad export e import se pueden elegir de manera selectiva los objetos o usuarios del archivo de volcado que se deseen importar, después import tratará de de insertar esos datos en la DB (en lugar de sobrescribir los registros existentes.

- Las exportaciones completas del sistema leen las tablas completas del diccionario de datos, además de los datos de aplicación. Las exportaciones completas del sistema pueden utilizarse para reconstruir completamente una base de datos, puesto que el diccionario de datos registra información sobre usuarios, los archivos de datos y objetos e la base de datos.

10. Protección contra software malicioso

Objetivo: Proteger la integridad de la información, de los registros y el hardware que conforman las bases de datos de la organización.

- Se deben tomar precauciones para prevenir, detectar la introducción de software malicioso por parte del personal interno y externo a la organización.

- Se debe concientizar a los usuarios sobre de los peligros del uso de software no autorizado o malicioso, los DBA y los Administradores de Redes deben introducir controles para detectar o prevenir la introducción de software malicioso. Principalmente se deben tener cautelas al detectar y prevenir la introducción de virus informáticos en computadoras personales.

10.1. Controles contra software malicioso

- La protección contra software malicioso debe fundamentarse en concienciar al personal en aspectos de seguridad y en la aplicación de adecuados controles de acceso al sistema y la administración de cambios.

- Se deben implementar controles de detección y prevención para la protección contra software malicioso, y procedimientos adecuados de concientización de usuarios. Se deben tener en cuenta: estas políticas deben estar diseñadas para servidores de archivos de red que brindan soporte a un gran número de estaciones de trabajo.

- Debe requerirse el uso de software con licencia y que a la vez se prohíba el uso de software no autorizado.

- Se debe proteger el los servidores y los SGDB contra los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando qué medidas de protección deberían tomarse.

- Se debe mantener una instalación y actualización periódica de software de detección, reparación anti-virus, para examinar computadoras y medios informáticos, como controles; preventivos, detectivos o correctivos.

- Se deben realizar revisiones periódicas del contenido de software y datos de los SGBD que sustentan procesos críticos de al empresa. La presencia de archivos no aprobados o modificaciones no autorizadas debe ser investigada formalmente por parte de la persona encargada de esta actividad o el DBA.

- Se deben verificar de la presencia de virus en archivos recibidos a través redes no confiables o en medios magnéticos de origen incierto o no autorizado, antes de su uso

- Se debe llevar a cabo una verificación de software malicioso en mensajes de correo electrónico y archivos descargados por Internet ("downloads"), esto antes de su uso; dicha verificación debe realizarse en diferentes lugares: en computadoras de escritorio, servidores de correo electrónico, o al ingresar en la red de la organización.

- Procedimientos y responsabilidades gerenciales para administrar la protección contra virus en los sistemas, el entrenamiento con respecto a su uso, la comunicación y la recuperación frente a ataques.

- Elaborar adecuados planes de continuidad de los negocios para la recuperación respecto de ataques de virus, incluyendo todos los datos necesarios, el resguardo del software y las disposiciones para la recuperación.

- Los gerentes deben garantizar que se utilizan fuentes calificadas de actualización de listas de virus, por ejemplo; publicaciones acreditadas, sitios de Internet o proveedores de software anti-virus confiables, para diferenciar entre virus falaces y reales.

- Se debe concientizar al personal acerca del problema de los virus falsos (hoax) y de las acciones a tomar al recibirlos.

- Se debe explicitar políticas claras en el uso del Internet y el correo electrónico, por ejemplo; prohibir la apertura de archivos adjuntos, prohibición de descargas de internet (downloads), etc.

10.2. Código troyano y canales ocultos

- El código troyano esta diseñado para afectar un sistema en una forma no autorizada, no fácilmente advertida y no requerida por el destinatario o usuario del programa.

- Un canal oculto puede exponer información contenida en las bases de datos utilizando algunos medios indirectos y desconocidos.

- Puede activarse modificando un parámetro accesible mediante elementos tanto seguros como no seguros de un sistema informático, o incorporando información a un flujo de datos. Los canales ocultos y el código troyano raramente surgen por accidente.

Si se aborda este tópico, se deben considerar los siguientes puntos:

- Solo comprar programas de proveedores acreditados
- Comprar programas en código fuente de manera que el mismo pueda ser
- verificado
- Utilizar productos evaluados
- Examinar todo el código fuente antes de utilizar operativamente el programa
- Controlar el acceso y las modificaciones al código una vez instalado el mismo
- Emplear personal de probada confiabilidad para trabajar en los sistemas críticos.

11. Mantenimiento

Objetivo: Mantener la integridad, la disponibilidad de los servicios de procesamiento en los SGBD y comunicación de la información de las bases de datos

- Se deben elaborar las estrategias más adecuadas de respaldos, back-Up, y copias de seguridad de él o los distintos SGBD, así como de la principal información de la organización.

- Se deben establecer y establecer procedimientos de rutina mediante los cuales se ensaye el restablecimiento oportuno, en el que se registren fallas, eventos y que además se monitoree el entorno del equipamiento.

- Cuando se crea un objeto de la base de datos (como una tabla o un índice) se debe asignar a un espacio de tablas mediante valores predeterminados de usuario o instrucciones específicas.

- Mediante la reconstrucción de índices se debe diseñar un programa de mantenimiento, para los índices que más utilicen en la base de datos.

- Se debe planificar periódicamente un trabajo por lotes para reconstruir los índices de las tablas más activas de una base de datos.

11.1. Resguardo de la información contenida en las bases de datos

- Se deben realizar periódicamente, de acuerdo a las necesidades, capacidad y crecimiento dinámico de las bases de datos de cada una de las organizaciones copias de respaldo de la información de las bases de datos así como de los sistemas de información y todo el software principal para la empresa.

- Se debe contar con apropiadas instalaciones de resguardo para garantizar que toda la información y el software esencial de la empresa puede recuperarse una vez ocurrido un desastre o falla de los dispositivos.

- Las instrucciones para el resguardo de cada uno de los SGDB deben ser ensayadas periódicamente para garantizar que cumplen con los requerimientos de los planes de continuidad de los negocios. Se debe tener en cuenta:

    - Se debe almacenar en una ubicación remota un nivel mínimo de información de respaldo, junto con registros completos y exactos de las copias de respaldo de los SGBD, y de los procedimientos documentados de restauración, se deben mantener a una distancia prudencial como para salvarlos de daños producidos por un desastre en el lugar principal. Se deben realizar y retener al menos tres generaciones o ciclos de información de resguardo de los SGBD y para las aplicaciones más significativas para la empresa.

    - Se debe asignar a la información de respaldo una cota apropiada de protección física y ambiental consecuente con los estándares utilizados en el lugar principal. Los controles aplicados a los dispositivos deben extenderse para cubrir también el lugar de resguardo.

- Los medios magnéticos de los respaldos deben probarse periódicamente, con la finalidad de garantizar la confiabilidad de los mismos en concordancia con su ocasional uso en casos de emergencia.

- También deben probarse y verificarse los procedimientos de restauración de los servidores y SGBD periódicamente para garantizar su eficacia y cumplimiento dentro del tiempo esperado para la recuperación en los procedimientos operativos.

- Se debe determinar el período de almacenaje de la información esencial de la empresa, y también los requerimientos de copias de archivos que han de guardarse en forma permanente.

- Se debe establecer un tiempo de vida útil para los medios de almacenamiento magnético de respaldos tales como CD's, cintas magnéticas, cartuchos, etc.

11.2. Registro de actividades del personal operativo

- Todo el personal operativo que utiliza las bases de datos de la organización debe mantener un registro de sus actividades.

  Ellos deben reportar:

  - Tiempos de inicio y cierre de la o las bases de datos

  - Errores del sistema y medidas correctivas ejecutadas

  - Confirmación del correcto manejo de archivos de datos y salidas (outputs)

  - Se debe prohibir, evitar o reducir la manipulación directa de los registros o datos directamente en a base de datos, todo cambio se lo debe realizar desde los sistemas, y en el último de los casos, esta manipulación debe ser realizada registrando todos y cada uno de los cambios ejecutados, quien lo ha realizado, etc.

  - Todo cambio que se realice a los sistemas y/o aplicaciones deben ser autorizados por el nivel Gerencial y supervisados por un encargado del área

  - Los registros de actividades del personal operativo deben estar sujetos a verificaciones periódicas e independientes con relación a los procedimientos operativos.

  - Se deben comunicar las fallas y tomar medidas correctivas. Se debe registrar las fallas comunicadas por los usuarios, con respecto a problemas con el procesamiento de la información o los sistemas de comunicaciones. Deben existir reglas claras para el manejo de las fallas comunicadas, con inclusión de:

  - Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente

  - Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron debidamente autorizadas.

12. Administración y seguridad de los medios de almacenamiento

Objetivo: Impedir el daño a los activos y las interrupciones en las actividades normales de la organización.

- Los diferentes medios de almacenamiento magnético deben ser controlados y protegidos físicamente, por ejemplo; almacenándolos en una caja fuerte ignífuga en un sitio prudentemente distante del sitio principal.

- Se deben implantar procedimientos operativos convenientes para proteger documentos, medios de almacenamiento (casetes, cintas, discos), datos de entrada/salida y documentación del sistema contra daño, robo y acceso no autorizado.

12.1. Administración de medios informáticos removibles

- Deben existir procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. Se deben considerar los siguientes lineamientos:

- Deben borrarse los contenidos previos de cualquier medio reutilizable que ha de ser retirado de la organización si ya no son necesarios.

- Se debe requerir autorización para retirar cualquier medio magnético de la organización y se debe realizar un registro de todos los retiros a fin de mantener una pista de auditoría.

- Todos los medios magnéticos de respaldo de información deben almacenarse en un ambiente protegido y seguro, de acuerdo con las especificaciones de los fabricantes o proveedores, conservando niveles de humedad y temperatura adecuados.

- Todos los procedimientos y niveles de autorización de retiro de medios magnéticos deben estar claramente documentados.

12.2. Procedimientos de manejo de la información

- Se deben implantar procedimientos para el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada.

- Los procedimientos de manejo de información deben elaborarse según la clasificación de la misma en comunicaciones móviles, redes, documentos, correo, sistemas informáticos, computación móvil, correo de voz, comunicaciones de voz en general, multimedia, instalaciones postales y servicios, uso de máquinas de fax y cualquier otro ítem sensible, por ejemplo; facturas y cheques en blanco.

Se deben considerar:

- Administración y rotulado de todos los medios magnéticos.
- Establecer limitaciones de acceso para identificar al personal no autorizado.
- Se debe mantener un registro formal de los receptores acreditados de datos.
- Se deben almacenar los medios magnéticos en un ambiente que concuerda con las especificaciones de los fabricantes o proveedores.
- Se debe garantizar que los datos de entrada a las bases de datos son completos, que el procesamiento se lleva a cabo correctamente y que se aplica la validación de salidas.
- Marcación clara de todas las copias de datos a fin de ser advertidas por el receptor autorizado.
- revisión de listados de distribución y de receptores autorizados a intervalos regulares.
- Proteger los datos en espera ("spooled data") los mismos que deben estar de acuerdo con el grado de sensibilidad de los mismos.
- Mantener la distribución de datos en un nivel mínimo.

12.3. Seguridad de la documentación del SGDB

La documentación del SGDB puede contener información sensible, por ejemplo; descripción de procesos de bases de datos, estructuras de datos, procedimientos, gestión de roles y privilegios, procesos de autorización de cambios, etc. Se deben tomar en cuenta las siguientes revisiones para proteger la documentación del SGDB de accesos no autorizados.

- La documentación del SGDB debe ser almacenada en forma y sitio seguros.
- La documentación del SGDB almacenada en una red pública, o suministrada a través de una red pública, debe ser protegida de manera adecuada
- El listado de accesos a la documentación del SGDB debe restringirse al mínimo y debe ser autorizado por el DBA o en su defecto por la gerencia.

13. Intercambios de información y software

Objetivo: Impedir la pérdida, uso inadecuado o modificación de la información que se intercambia entre organizaciones.

- Estos intercambios deben ser controlados y deben ir de la mano con la legislación aplicable y deben realizarse en conformidad con los acuerdos existentes.
- Se deben establecer procedimientos y estándares para proteger la información y los medios en tránsito.
- Se deben considerar las implicaciones comerciales y de seguridad relacionadas con el intercambio electrónico de datos, el comercio electrónico y el correo electrónico, además de los requerimientos de controles.

13.1. Acuerdos de intercambio de información y software entre organizaciones

- Para el intercambio de información y/o de software (de forma electrónica y/o manual) entre organizaciones, se deben instaurar acuerdos, algunos de ellos pueden ser formales, y pueden incluir acuerdos de custodia de software cuando corresponda.
- Los detalles de seguridad de los convenios de esta índole deben reflejar el grado de sensibilidad de la información de negocio involucrada.
- Los convenios sobre requerimientos de seguridad deben tener en cuenta: responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.

  Se debe:

  - Instaurar procedimientos de notificación de emisor, transmisión, envío y recepción
  - Establecer esquemas técnicos mínimos para armado de paquetes y transmisión
  - Establecer estándares de identificación de mensajeros ("couriers")
  - Implantar responsabilidades y obligaciones en caso de pérdida de datos.
  - Uso de un sistema convenido para el rotulado de información crítica o sensible, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida
  - Conseguir detalles sobre la propiedad de la información y el software, y responsabilidades por la protección de los datos, el cumplimiento del "derecho de propiedad intelectual" del software y consideraciones similares
  - Establecer estándares técnicos para la grabación y lectura de la información y software
  - Implementar controles especiales que pueden requerirse para proteger ítems sensibles, como las claves criptográficas.

13.2. Seguridad de los medios en tránsito

La información contenida en medios magnéticos de almacenamiento (cintas, cartuchos, Cd's que contienen respaldos, backups, etc.), pueden estar expuestas a accesos no autorizados, y están propensos al mal uso o alteración durante el transporte físico, por ejemplo; cuando se los envía a través de servicios postales, correo o mensajería.

- Se deben ejecutar controles y éstos deben ser aplicados con la finalidad de proteger los medios informáticos que se transportan entre distintos puntos.
- Se deben recurrir a medios de transporte o servicios de mensajería confiables.
- Se debe concertar con la gerencia un listado de servicios de mensajería autorizados e efectuar un procedimiento para verificación e identificación de los mismos.
- El embalaje a utilizar debe ser lo suficientemente seguro como para proteger el contenido contra imprevistos daños físicos mientras se encuentra en tránsito y se debe seguir las especificaciones de los fabricantes o proveedores.
- Se deben adoptar controles especiales para proteger la información sensible contra divulgación o modificación no autorizadas. Entre las mejores prácticas a adoptar están;

  1) Entrega en la mano
  2) Uso de recipientes cerrados;
  3) Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso)
  4) En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

14. Políticas de control de accesos a bases de datos

Objetivo: Controlar el acceso a la información contenida en las bases de datos de la organización.

- Los requerimientos de negocio para el control de accesos se deben definir y documentar obligatoriamente.
- Los accesos a las bases de datos y a su información en los procesos del negocio deben ser controlados en base a los requerimientos la seguridad y su gestión.
- Se deben definir, documentar las reglas y derechos del control de accesos para cada usuario y/o grupo de usuarios.
- Se debe otorgar a los usuarios y proveedores de servicio una clara enunciación de los requerimientos comerciales que deberán satisfacer los controles de acceso.

  La política debe contemplar lo siguiente:

  - Se deben establecer los requerimientos de seguridad de los SGBD de una manera formal y documentada.
  - Se debe Identificar toda información relacionada con las aplicaciones comerciales.
  - Se deben establecer los principios de no divulgación y autorización de información, también el principio de necesidad de conocer, los niveles de seguridad y la clasificación de la información de la organización.
  - Deben funcionar correlacionadamente las políticas de control de acceso y las de clasificación de información de los diferentes sistemas y redes.
  - La legislación debe ser aplicable y resaltar con las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
  - Obligatoriamente de deben establecer perfiles de acceso de usuarios estándar.
  - La administración de derechos de acceso debe ser elaborada en un ambiente distribuido y de red que reconozcan todos los tipos de conexiones disponibles.
  - Los roles deben ser establecidos en forma clara y específica, asignando el nivel de acceso respectivo a los usuarios o grupos de usuarios, definiendo a cuales objetos pueden acceder y a los datos que está autorizado su acceso.

15. Políticas de control de accesos a las bases de datos para administradores y usuarios de bases de datos

Objetivo.- Diferenciar entre políticas de control de accesos obligatorias y políticas optativas o condicionales.

15.1. Políticas de control de accesos obligatorias para Administradores de bases de datos:

- Los roles, perfiles y claves de acceso para usuarios serán generados, controlados y administrados por el DBA de la organización. Y además éstos deberán ser autorizados por el nivel gerencial de la organización.
- El DBA de la organización será la persona encargada de restringir y eliminar roles, perfiles de usuario y cuentas comprometidas y/o revocadas.
- El DBA debe ser el encargado de conservar y garantizar mediante la ejecución de procedimientos y el uso de herramientas propias del SGBD u otras la confidencialidad, integridad y la disponibilidad de las bases de datos.
- El DBA debe gestionar mediante procesos de SGBD la renovación, revocatoria de contraseñas de usuarios.
- Los accesos fallidos a las bases de datos deben bloquear la misma luego del tercer intento.
- Las claves de acceso deben contener caracteres alfanuméricos y su longitud mínima debe ser conformada por al menos 11 caracteres de manera recomendable y segura.
- En los SGDB que contengan procesos de caducidad, se debe establecer la calendarización para la expiración para claves de acceso en forma particular para cada usuario.

15.2. Políticas de control de accesos condicionales / optativas para administradores de bases de datos:

- El DBA debe anular y/o revocar las cuentas de usuario desde las que hayan intentado o se intenten accesos no autorizados a las bases de datos.
- El DBA debe cambiar y/o modificar los claves de acceso de los usuarios de la base de datos si ellas se encuentran comprometidas.
- Queda completamente prohibido el acceso a otras bases de datos y aplicaciones de la organización, este acceso sólo esta permitido hasta donde los niveles de privilegios y perfiles de cada usuario lo determinen.
- Se debe coordinar con la gerencia de la organización el tipo y las sanciones para el personal que accidental o planificadamente perpetre en accesos no autorizados a las bases de datos.

15.3. Registración de usuarios

- Se debe establecer un procedimiento formal de registración y desregistración de usuarios para otorgar acceso a las bases de datos y prestaciones de información multi-usuario. El acceso a servicios de información multi-usuario debe ser controlado a través de un proceso formal de registración de usuarios, el cual debe incluir los siguientes puntos:

- Se debe utilizar ID's de usuario únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones.

- El uso de ID's grupales debe ser verificado y sólo deben ser autorizados cuando van a ser usados en alguna actividad de trabajo como:

- Entregar e informar a los usuarios un detalle escrito de sus derechos de acceso.

- Demandar que los usuarios firmen una declaración señalándoles las condiciones para el acceso.

- Comprobar que el nivel de acceso a las bases de datos y sistemas de información concedido es adecuado y se ajusta al proyecto del negocio y está ligado con la política de seguridad de la organización.

- Validar a los usuarios tiene autorización del DBA para el uso del SGDB o servicio de información. Puede requerirse en ciertos casos la aprobación de acceso por parte de la gerencia.

- Garantizar que el DBA no otorgue accesos a las bases de datos hasta que se hayan completado los procedimientos de autorización.

- Mantener un registro formal de todas las personas autorizadas a utilizar los servicios.

- Invalidar inmediatamente los derechos de acceso de los usuarios que han cambiado sus tareas o se desvincularon de la organización.

- Controlar y verificar periódicamente un historial de privilegios, roles y usuarios dados de baja y/o redundantes.

- Verificar periódicamente, y cancelar ID's y cuentas de usuarios redundantes; garantizar que los ID's de usuario redundantes no se reasignen a otros usuarios.

Se deben especificar cláusulas en los contratos de personal (usuarios de la base de datos) en las que se especifiquen sanciones disuasivas que se adoptarán en contra de intentos de accesos no autorizados a las bases de datos.

15.4. Administración de privilegios de usuario

Se debe limitar, controlar la asignación de privilegios de acceso y uso de las bases de datos de la organización que permitan que el usuario omita controles de acceso, ya que el uso inadecuado de los privilegios resulta usualmente en uso malintencionado de las bases de datos afectando a su seguridad.

Las bases de datos que requieren protección contra accesos no autorizados, deben prever una concesión de privilegios controlada mediante un proceso de autorización formal. Se debe tener en cuenta lo siguiente:

- Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados.
- Los privilegios deben asignarse con una identidad de usuario diferente de aquellas utilizadas en las actividades normales.
- Los niveles de privilegios deben asignarse de acuerdo a la necesidad y a la actividad que van a realizar de los usuarios de las bases de datos.
- Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización de los mismos.
- Se debe promover el desarrollo y uso de rutinas del SGDB para evitar la necesidad de otorgar privilegios a los usuarios.

15.5. Administración de contraseñas de usuario

Las contraseñas sirven para verificar y validar la identidad de un usuario para acceder a bases de datos o servicios de información. Se debe establecer un proceso de administración formal en la asignación de contraseñas, mediante el cual debe realizar lo siguiente:

- Se debe establecer que las contraseñas provisorias que se asignan a los usuarios que olvidan las mismas, solo debe suministrarse una vez identificado el usuario.
- Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro), se debe cifrar el password previo al envío del archivo y obligatoriamente los usuarios deben acusar recibo de la recepción de la clave (password).
- Las contraseñas nunca deben ser almacenadas en sistemas informáticos sin protección.
- Se deben generar contraseñas provisorias seguras para otorgarlas a los usuarios de las bases de datos.
- Los usuarios de bases de datos solamente serán asignados para los sistemas o para los administradores de los SGDB.

15.6. Revisión de derechos de acceso de usuario de las bases de datos

Para lograr mantener un control eficaz del acceso a las bases de datos y servicios de información, de la organización debe llevarse a cabo un proceso periódico y formal de revisión de los derechos de acceso de los usuarios, de forma que:

- Las asignaciones de privilegios y roles de usuario se verifiquen a intervalos regulares, a fin de garantizar que no se obtengan privilegios y/o roles no autorizados.

- Los derechos de acceso de los usuarios se revisen a intervalos regulares (se recomienda cada fin de mes) y después de cualquier cambio realizado.

- Las autorizaciones, derechos de acceso y privilegios especiales se deben revisar a intervalos más cortos y frecuentes.

- Los usuarios autorizados al uso de las bases de datos de la organización deben prestar toda su cooperación y comprometerse con la organización con el objetivo de lograr la eficacia de la seguridad de la información y el buen uso de las bases de datos.

- Se debe sensibilizar a los usuarios acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad de la información contenida en las bases de datos.

15.7. Uso de contraseñas

- Los usuarios deben seguir buenas prácticas de seguridad, conservación y el uso de contraseñas de acceso a las bases de datos de la organización.

- Las contraseñas establecen un medio de validación de la identidad de un usuario y consecuentemente un medio para constituir derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben tener presente lo siguiente:

- Conservar las contraseñas en secreto.

- No compartir las contraseñas individuales de usuario.

- Evitar mantener un registro de contraseñas en papel, a menos que este pueda ser almacenado en forma segura.

- Cambiar las contraseñas siempre que exista un posible indicio de compromiso del o los SGDB o de sí mismas

- Seleccionar contraseñas de calidad, con una longitud mínima de seis caracteres que:

    1) Sean fáciles de recordar.

    2) No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo; nombres, números de teléfono, fecha de nacimiento, etc.

    3) No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

- Cambiar las contraseñas a intervalos regulares o según el número de acceso (las contraseñas de cuentas con privilegios deben ser modificadas con mayor frecuencia que las contraseñas comunes), y evitar reutilizar o reciclar viejas contraseñas.

- Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").

- No incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo; aquellas almacenadas en una tecla de función o macro.

- Si los usuarios necesitan acceder a distintas bases de datos y se requiere que mantengan múltiples contraseñas, se debe notificar a los mismos que pueden utilizar una contraseña de calidad única para todos los servicios que brinden un nivel razonable de protección de las contraseñas almacenadas.

16. Control de acceso a bases de datos

Objetivo: Imposibilitar los accesos no autorizados a la información contenida en las bases de datos y sistemas de información de la organización.

- Las herramientas de seguridad deben ser usadas para delimitar los accesos no autorizados a los SGDB.

- El acceso lógico a los SGDB y a la información debe estar limitado a los usuarios autorizados.

Los SGDB deben:

- Tener la capacidad de otorgar acceso a las bases de datos de la organización a los individuos que estén debidamente autorizados mediante designación formal, o a grupos bien definidos de usuarios.

- No comprometer la seguridad de las bases de datos y otros sistemas con los que se comparten recursos de información.

- Controlar el acceso de usuarios a la información y a las funciones de los SGDB, de acuerdo con la política de control de accesos definida por la organización.

- Brindar protección contra el acceso no autorizado a las bases de datos y software del sistema operativo que tengan la capacidad de pasar por alto los controles de sistemas o aplicaciones.

16.1. Restricción del acceso a la información contenida en las DB's

- Los usuarios de bases de datos, incluido el personal de soporte, deben tener acceso restringido a ia información y a las funciones de los SGDB de acuerdo al criterio del DBA de la organización.

Para brindar apoyo a los requerimientos de limitación de accesos, se debe considerar la aplicación de los siguientes controles:

- Se deben controlar los accesos a las funciones de los SGDB mediante la provisión de menús.

- Restricción del conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no estén autorizadas para su acceso, con la adecuada edición de documentación de usuario.

- Control de los derechos de acceso de los usuarios, por ejemplo; lectura, escritura, supresión y ejecución.

- Garantizar que las salidas (outputs) de los sistemas de aplicación que administran información sensible, contengan solo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas, y revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

16.2. Aislamiento del SGDB

Los sitios en los que funcionan las bases de datos de las organizaciones requieren de un ambiente informático dedicado (aislado). Los SGDB son muy susceptibles a perdidas potenciales y por ello requieren un tratamiento especial. Sólo debe compartir recursos con los sistemas de aplicación confiables.

Se deben realizar las siguientes consideraciones:

- Si se requiere compartir recursos, los SGDB y las aplicaciones sensibles han de ejecutarse en un ambiente compartido, los SGDB y los sistemas de aplicación con los cuales esta compartirá los recursos deben ser identificados y acordados con el propietario de la aplicación sensible.

- La sensibilidad de un SGDB debe ser claramente identificada y documentada por el DBA de la organización y/o el personal encargado.

17. Monitoreo del acceso y uso de bases de datos

Objetivo: Detectar actividades no autorizadas realizadas en las bases de datos de la organización.

- Los SGDB deben ser monitoreados para descubrir desviaciones que vayan en contra de la política de control de accesos y también se deben registrar eventos para proporcionar evidencia(s) en caso de producirse incidentes inherentes a la seguridad.

- El monitoreo de los SGDB permite evidenciar la eficacia de los controles adoptados y verificar su acuerdo con el correspondiente modelo de política de accesos.

17.1. Registro de eventos

- En los SGDB de la organización, deben generarse registros de auditoría que contengan eventos relativos a seguridad, excepciones, etc. y deben conservarse por un período definido para acceder en las futuras investigaciones y en el monitoreo de control de accesos.

  Estos registros de auditoría deben incluir:

  - Fecha y hora de inicio y terminación de la sesión.
  - ID de usuario.
  - Registros de intentos exitosos fallidos de acceso al sistema.
  - Registros de intentos exitosos y fallidos de acceso a datos, así como otros
  - recursos.
  - Identidad o ubicación de la terminal, si fuese dable.

Los registros de auditoría que hayan presentado novedades deben ser archivados y deben formar parte de la política de retención de registros o a los requerimientos de recolección de evidencia.

17.2. Protección de los registros de las bases de datos de la organización

- Los registros que forman parte de las bases de datos de la organización, deben protegerse contra pérdida, destrucción y falsificación.

- Se puede requerir una segura retención de varios registros para cumplir requerimientos normativos o legales, así como para respaldar actividades esenciales del negocio. Podría suceder por ejemplo; que los registros de las DB's puedan solicitarse como prueba de que una organización opera dentro de un determinado marco legal o normativo, o para asegurar una buena protección contra imprevistas acciones penales, civiles o para conocer el estado financiero de una organización frente a auditores, socios y accionistas.

- Se deben mantener y conservar en forma segura las claves criptográficas asociadas con archivos cifrados o firmas digitales. Éstas claves criptográficas deben estar disponibles para su uso por parte de personas autorizadas cuando su uso fuese requerido

- Los procedimientos de almacenamiento y manipulación deben implementarse de acuerdo con las recomendaciones del fabricante. Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros.

- Se deben incluir procedimientos para garantizar la capacidad y el acceso a los datos contenidos en medios de almacenamiento electrónicos (tanto en la legibilidad de los datos como en medios), para salvaguardar los mismos contra eventuales pérdidas ocasionadas por posibles cambios en la tecnología.

- Se deben seleccionar los sistemas de almacenamiento de datos manera que los datos solicitados puedan recuperarse de un modo aceptable en el caso de que un tribunal de justicia los solicite, por ejemplo; que todos los registros de la base de datos necesitados se logre recuperar en un plazo y un formato aceptable.

- Los registros deben ser clasificados en diferentes tipos, por ejemplo; registros de base de datos, "logs" de transacciones, "logs" de auditoría y procedimientos operativos, individualmente se detallará el tipo de medios de almacenamiento utilizados, los períodos de retención y, por ejemplo; papel, microfichas, medios magnéticos u ópticos

- Se debe garantizar el sistema de almacenamiento y manipulación, mediante una clara identificación de los registros y de su período de retención normativa o legal. Si los registros ya no resultasen necesarios para la organización debe permitirse una adecuada destrucción de los mismos.

Para lograr cumplir con estos compromisos, se deben tomar las siguientes medidas dentro de la organización.

- Se debe mantener un inventario de fuentes de información clave

- Se deben emitir lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información de las bases de datos de la organización

- Se deben implementar controles esenciales contra pérdida, destrucción y falsificación; para proteger los registros y la información contenida en las bases de datos de las organizaciones.

- Se debe preparar un cronograma de retención de registros identificando sus tipos y el período por el cual deben ser retenidos.

17.3. Protección de datos y privacidad de la información personal

- Cabe mencionar que en el Ecuador las leyes referentes a la Jurismática, todavía se encuentran en estudio y los párrafos subsiguientes encontrados en la Web, están citados como proyectos de ley.

- "Doctrinariamente el Hábeas Data protege a la integridad moral de las personas, frente a informaciones referidas a su personalidad, tales como: su afiliación política,

gremial, religiosa, su historia laboral, sus antecedentes crediticios, policiales e informaciones similares que constan en registros o bancos de datos. Es una garantía que protege varios derechos, tales como, la honra, la buena reputación, la intimidad y también el derecho a la información. *En la Constitución que entró en vigencia el* ***10 de agosto de 1998****, la cual fue reformada y codificada por la Asamblea Nacional constituyente, se estable que:*

Art. 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.

Podrá solicitar ante el funcionario respectivo, la actualización de los datos o sus rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

El texto vigente hasta el 09 de agosto de 1998, disponía en el artículo 30 inciso segundo:

Igualmente, podrá solicitar ante el funcionario o Juez competente la actualización, rectificación, eliminación o anulación de aquellos si fueren erróneos o afectaren ilegalmente sus derechos".[2]

- Se debe conservar y manejar con la cautela del caso la (información sobre personas vivas), la misma que puede ser identificada para ser tratada de acuerdo a las leyes nacionales ya que muchos países han incluido en sus leyes controles sobre el procesamiento y transmisión de datos personales.

- Generalmente se debe asignar un responsable para la protección de datos, el mismo debe orientar a los usuarios, y prestadores de servicios a cerca de las responsabilidades y procedimientos a seguirse.

- Debe ser responsabilidad del dueño de los datos, informar al responsable de la protección de los mismos sobre las propuestas para conservar la información personal en un archivo estructurado, y para garantizar la comprensión de los principios de protección de datos, definidos en la legislación pertinente.

17.4. Prevención del uso inadecuado de los recursos de procesamiento de información

- El uso de las bases de datos de la organización deben ser autorizados por la gerencia, así como de los recursos de información contenidos en las bases de datos de la empresa. Los recursos de procesamiento de información de una organización se suministran con propósitos de negocio.

- La utilización de los recursos de procesamiento de información con propósitos no autorizados o ajenos a los negocios, sin la aprobación de la gerencia, debe ser considerada como de uso indebido. Si dicha actividad es identificada mediante monitoreo u otros medios, se debe notificar al gerente interesado para que se tomen las acciones disciplinarias que correspondan.

- Se debe hacer uso de controles disuasivos en la legalidad del monitoreo del uso de los recursos de información y puede requerir que los empleados sean advertidos de dichas actividades o que se obtenga el consentimiento de los mismos.

- Se debe obtener asesoramiento jurídico antes de la implementación de procedimientos de monitoreo.

- Es esencial que los usuarios estén al corriente del alcance que tienen los accesos permitidos ya que el uso de inadecuado de los recursos informáticos puede constituir un delito criminal, esto según las normativas y leyes de cada país. Para ello las autorizaciones de las debe conceder y autorizar por escrito; y una copia de la misma debe ser firmada por los usuarios también retenida en forma segura por la organización.

- Los usuarios y empleados externos deben ser advertidos sobre la clara prohibición de no realizar accesos no autorizados.

- En las bases de datos de la organización, en el instante que se inicia una sesión debe aparecer un mensaje de advertencia en pantalla indicando que la aplicación a la que se está accesando es privada y que no se permite el acceso no autorizado. El usuario debe acusar recepción y responder en forma apropiada al mensaje para continuar con el proceso de inicio de sesión.

18. Administración de la red

Objetivo: Garantizar la seguridad de la información en las redes y la protección de la infraestructura de apoyo.

- Es de vital importancia la administración de seguridad de las redes que pueden atravesar el perímetro de la organización, estas deben estar adecuadamente protegidas.

- Deben establecerse controles adicionales para los datos e información sensible que circulen y se transfieran por redes públicas, por ejemplo el uso de criptografía.

18.1. Controles de redes

- Se requiere un conjunto de controles para lograr y mantener la seguridad de las redes informáticas.

- Los administradores de redes deben implementar controles para garantizar la seguridad de los datos en la misma, y la protección de los servicios conectados contra el acceso no autorizado.

Se debe considerar:

- La responsabilidad operativa de las redes debe estar separada de las de operaciones de el o los PC's.

- Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.

- También pueden requerirse controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

- Se deben instituir procedimientos y responsabilidades para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias.

- Las actividades gerenciales deben estar estrechamente coordinadas tanto para optimizar el servicio a la actividad de la empresa cuanto para garantizar que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

19. Control de acceso a la red

Objetivo: Proteger los servicios de red de la organización.

- Se debe asegurar los acceso la red tanto internos como externos, para de esta manera asegurar que los usuarios que tengan acceso a las redes, a sus servicios y no comprometan la seguridad de la misma, garantizando:

  a) Interfaces inadecuadas entre la red de la organización, redes públicas o redes de otras organizaciones.

  b) Dispositivos de autenticación apropiados el equipamiento y usuarios.

  c) Control en el acceso de usuarios a los servicios de información.

19.1. Ruta forzada

Objetivo: Evitar que los usuarios seleccionen rutas fuera de la trazada entre la terminal de usuario y los servicios a los cuales el mismo está autorizado a acceder.

Puede ser necesario controlar la ruta desde el terminal de usuario hasta el servicio informático. Las redes son diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad de ruteo. Estas características pueden ofrecer oportunidades para el acceso no autorizado a las bases de datos o a las aplicaciones de negocios, o para el uso no autorizado de servicios de información:

- Se debe establecer la finalidad del uso de una ruta forzada, la cual es impedir que los usuarios escojan rutas fuera de la trazada entre la terminal de usuario y los servicios a los cuales el mismo esta autorizado a acceder.

- Se debe delinear el control de ruta desde la terminal de usuario hasta el servidor de bases de datos. Las redes están delineadas para permitir un máximo alcance de distribución de recursos y flexibilidad de ruteo. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las bases de datos de las organizaciones, o para el uso no autorizado de sistemas de información.

- Se deben reducir los riesgos mediante la instauración de controles, mismos que limiten la ruta entre una terminal de usuario y los servidores de bases de datos, a los cuales sus usuarios están autorizados a acceder, por ejemplo creando un camino forzado.

- Se deben limitar las opciones de ruteo en cada punto de red, a través de elecciones predefinidas, como por ejemplo;

- Evitar la navegación ilimitada por la red.

- Instituir dominios lógicos separados para restringir el acceso a la red, por ejemplo; establecer redes privadas virtuales para grupos de usuarios dentro de la organización.

- Implantar el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.

- Asignación de números telefónicos o líneas dedicadas.

- Limitar las opciones de menú y submenú de cada uno de los usuarios.
- Conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
- Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo; firewalls.

19.2. Subdivisión de redes

- Cuando se requiera interconexión de la organización con otras sociedades o para su uso compartido de instalaciones de procesamiento de información y redes, se deben mitigar los riesgos; como el acceso no autorizado a los servidores y a las bases de datos ya existentes que utilizan la red. Dichas extensiones podrían requerir protecciones contra otros usuarios de la red y su finalidad es la de segregar grupos de servicios de información, usuarios y sistemas de información.
- Para controlar la seguridad de redes extensas se las debe dividir en dominios lógicos apartados, por ejemplo; dominios de red internos y externos de una organización, cada uno protegido por un perímetro de seguridad definido, el mismo que puede ser implementado mediante la instalación de una compuerta ("gateway") segura entre dos redes que han de ser interconectadas, para controlar el acceso y flujo de información entre los dos dominios. Este "gateway" debe ser configurado para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo con la política de control de accesos de la organización, ejemplo; "firewall".
- Los criterios para la subdivisión de redes en dominios deben basarse en la política de control de accesos, los requerimientos de acceso, tomar en cuenta el costo relativo y el impacto del desemzpeño que ocasiona la incorporación de un ruteador de red o una tecnología de "gateways" adecuados.
- Los requerimientos relativos a enrutamientos forzados deben basarse en la política de control de accesos de la organización.

19.3. Autenticación de usuarios para conexiones externas

- El acceso de usuarios remotos debe estar sujeto a la autenticación, ya que las conexiones externas son una alta oportunidad para que se realicen acceso no autorizados a la información de la empresa, por ejemplo el acceso mediante discado.
- Se pueden utilizar métodos de autentificación fuertes como el uso de técnicas criptográficas que brindan un mayor grado de protección que otros. Es importante determinar mediante una evaluación de riesgos el nivel de protección requerido. Esto es necesario para la adecuada selección del método.
- La autenticación de usuarios remotos puede llevarse a cabo utilizando, por ejemplo, una técnica basada en criptografía, "tokens" de hardware, o un protocolo de pregunta/respuesta.
- Deben también utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

- Los controles y procedimientos de rellamada o dail-back utilizando módems, pueden brindar protección contra conexiones no autorizadas y no deseadas a las instalaciones de procesamiento de información de la organización, este tipo de control autentica a los usuarios que intentan establecer una conexión con una red de la organización desde locaciones remotas. Al aplicar este control, la organización no debe utilizar servicios de red que incluyan desvío de llamadas o, si lo hacen, deben inhabilitar el uso de dichas herramientas para evitar las debilidades asociadas con la misma. Asimismo, es importante que el proceso de rellamada garantice que se produzca una desconexión real del lado de la organización. De otro modo, el usuario remoto podría mantener la línea abierta fingiendo que se ha llevado a cabo la verificación de rellamada.

Los procedimientos y controles de rellamada deben ser probados exhaustivamente respecto de esta posibilidad.[1]

19.4. Autenticación de nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para acceder sin autorización a una aplicación de la organización. Por ello;

- Se debe propender a que las conexiones a bases de datos y sistemas informáticos remotos sean seguras, éstas deben ser necesariamente autenticadas. Esto es particularmente importante si la conexión utiliza una red que esta fuera de control de la gestión de seguridad de la organización.

- La autenticación de nodos debe servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

19.5. Protección de los puertos de diagnóstico remoto

- El acceso a los puertos de diagnóstico debe ser controlado de manera segura.

- Se debe evitar accesos no autorizados a las bases de datos de la organización y para ello se deben proteger y controlar de una manera segura los puertos de diagnóstico mediante un mecanismo de seguridad apropiado, por ejemplo; una cerrojo de seguridad y una manera que garantice al acceso al personal de hardware y software aprobado por el gerente de recursos informáticos de la organización.

19.6. Control de conexión a la red

- Se debe limitar la capacidad de conexión de usuarios con redes externas que se extienden más allá de los límites de la organización mediante controles como "gateways" de red que filtren el tráfico mediante reglas o tablas previamente definidas. Las prohibiciones aplicadas deben basarse en la política y los requerimientos de accesos de las bases de datos de la organización.

Entre las aplicaciones que deben aplicarse restricciones están:

a) transferencia de archivos en ambas direcciones.

b) acceso interactivo.

c) acceso de red vinculado a hora o fecha.

d) correo electrónico.

e) transferencia unidireccional de archivos.

19.7. Control de ruteo de red

- Los controles de ruteo deben basarse en la verificación positiva de direcciones de origen y destino.

- Las redes compartidas con otros organismos e instituciones, especialmente aquellas que se extienden más allá de los límites organizacionales, deben requerir la agregación de controles de ruteo para avalar que las conexiones y los flujos de información no vulneren la política de control de acceso de las aplicaciones comerciales.

- Se debe realizar el aislamiento de redes y evitar que se propaguen desde la red de una organización a una red de otra mediante la traducción de direcciones y estas pueden implementarse en software o hardware.

19.8. Seguridad de los servicios de red

Las organizaciones deben garantizar que utilizan en sus servicios de red, se provea de una clara descripción de los atributos de seguridad de todos los servicios utilizados.

20. Control de acceso al sistema operativo

Objetivo: Impedir el acceso no autorizado al servidor de bases de datos y sistemas de información.

- A nivel de sistema operativo los mecanismos de seguridad deben ser utilizados para limitar el acceso a los recursos de los servidores, estas facilidades deben tener la capacidad de llevar a cabo:

- Se deben restringir los tiempos de conexión de los usuarios a un horario normal de labores, según corresponda.

- Se debe identificar, verificar la identidad, la ubicación y, si fuera necesario, la terminal de cada usuario autorizado a acceder al sistema.

- Se deben registrar los accesos exitosos y fallidos al sistema.

- Mediante la utilización de un sistema de administración de contraseñas se deben suministrar medios de autenticación apropiados, y éste debe asegurar la calidad de las mismas.

20.1. Identificación automática de terminales

- Debe ser necesaria la identificación automática de terminales para autenticar conexiones a los SGDB, servidores y a equipos portátiles.

- Se debe utilizar identificación automática de terminales ésta técnica puede utilizarse si resulta importante que la sesión solo pueda iniciarse desde una terminal o una ubicación determinadas.

- Debe utilizarse un identificador de la terminal, o adjunto a la misma, para indicar si esta terminal especifica esta autorizada a iniciar o recibir ciertas transacciones.

- Es necesario asignar protección física a las terminales, a fin de mantener la seguridad del identificador de la misma.

20.2. Procedimientos de conexión de terminales

- El acceso a los servicios de información de las bases de datos deben ser posibles mediante un proceso de conexión seguro.

- El procedimiento de conexión en un SGBD debe ser diseñado para minimizar la oportunidad de acceso no autorizado.

- Se debe divulgar información mínima posible acerca del SGDB, a fin de evitar dar apoyo innecesario a un usuario no autorizado.

Un buen procedimiento de identificación debería:

- Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.

- No facilitar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.

- Desplegar la siguiente información al completarse una conexión exitosa.

1) Fechas y hora de la conexión exitosa anterior.

2) Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

- Desplegar un aviso general advirtiendo que solo los usuarios autorizados pueden acceder a las bases de datos de la organización.

- Limitar el número de intentos de conexión no exitosos (se recomiendan tres) y considerar:

1) Registrar los intentos de acceso no exitosos.

2) Implementar una tardanza obligatoria antes de permitir otros intentos de identificación, o rechazar otros intentos sin autorización especifica

3) Desconectar conexiones de data link

- No desplegar identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.

- Restringir los tiempos máximos y mínimos permitidos para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.

20.3. Identificación y autenticación de los usuarios

- Todos los usuarios de las bases de datos (personal de soporte técnico, operadores, administradores de red, programadores de sistemas y administradores de bases de datos), deben tener un identificador único (ID de usuario) asignado solamente para uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los ID's de usuario no deben dar ningún inicio del nivel de privilegio del usuario, por ejemplo; gerente, supervisor, etc.

- La aprobación por parte de gerencia para I y A debe estar documentada para circunstancias excepcionales, cuando existe un claro beneficio para la empresa, pueda utilizarse un ID compartido para un grupo de usuarios o una tarea especifica. Podrían requerirse controles adicionales para mantener la responsabilidad.

- Existen diversos procedimientos de autenticación, los cuales pueden ser utilizados para sustentar la identidad alegada del usuario. Las contraseñas constituyen un medio muy común para proveer la identificación y autenticación (I y A) sobre la base de un secreto que solo conoce el usuario. También se puede llevar a cabo lo mismo con medios criptográficos y protocolos de autenticación.

- Para (I y A), se debe utilizar objetos como tarjetas inteligentes "tokens" con memoria que poseen los usuarios también pueden utilizarse para identificación y autentificación.

- Para autentificar la identidad de una persona deben utilizarse también las tecnologías de autenticación biométrica, las mismas que utilizan las características o atributos únicos de un individuo.

- Para lograr una autentificación más fuerte se debe hacer uso de una combinación de tecnologías y mecanismos vinculados para hacer la autentificación más segura.

20.4. Sistema de administración de contraseñas

- Las contraseñas que van a ser usadas para acceder a las bases de datos por parte de los usuarios deben ser generadas y asignadas únicamente por el DBA de la organización.

- Las contraseñas generadas por el DBA deben ser generadas como contraseñas de calidad y deben ser de longitud fija.

- Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad como orientación acerca del uso de las mismas.

- Las contraseñas constituyen uno de los principales medios de validación de la autoridad y de privilegios que tiene un usuario para acceder a las bases de datos de la organización.

- Generalmente en empresas medianas y grandes los sistemas y aplicaciones requieren que las contraseñas de usuario sean asignadas por una autoridad independiente.

- En emperezas pequeñas por lo general las contraseñas son seleccionadas y mantenidas por los usuarios.

Un buen sistema de administración de contraseñas debe:

- Imponer una selección de contraseñas de calidad.

- No mostrar las contraseñas en pantalla, cuando son ingresadas.

- Imponer el uso de contraseñas individuales para determinar responsabilidades.

- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

- Cuando corresponda, permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso.

- Cuando los usuarios seleccionan contraseñas, obligarlos a cambiar las contraseñas temporarias en su primer procedimiento de identificación.

- Mantener un registro de las contraseñas previas del usuario, por ejemplo de los 12 meses anteriores, y evitar la reutilización de las mismas.

- Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.

- Modificar las contraseñas predeterminadas por el vendedor, una vez instalado el software.

20.5. Desconexión de terminales por tiempo muerto

- Se deben utilizar herramientas de desconexión por tiempo muerto, estas deben limpiar la pantalla de las terminales y deben cerrar tanto la sesión de la aplicación como la de red, después de un periodo definido de inactividad.

- El lapso por tiempo muerto debe responder a los riesgos de seguridad del área y de los usuarios de la terminal. Para algunas PC's, puede suministrarse una herramienta limitada de desconexión de terminal por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

- Con la finalidad de evitar el acceso de personas no autorizadas, las terminales inactivas en ubicaciones de alto riego, como; áreas externas o públicas fuera del alcance de la gestión de seguridad de la organización, deben apagarse después de un periodo definido de inactividad.

20.6. Limitación del horario de conexión

- El horario de conexión debe ser establecido y formalizado en un documento de funcionamiento de la organización.

- La conexión a las bases de datos de la organización estará permitido a los usuarios sólo en horario normal de trabajo.

- Las restricciones al horario de conexión deben suministrar seguridad adicional a las bases de datos y aplicaciones de alto riesgo de la organización.

- La limitación del periodo durante el cual se permiten las conexiones de terminal a los SGDB, reduce el espectro de oportunidades para el acceso no autorizado. Se debe considerar un control de esta índole para bases de datos, especialmente en aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo; áreas públicas o externas que estén fuera del alcance de la gestión de seguridad de la organización.

Entre las restricciones se pueden enumerar las siguientes:

- Su utilización debe ser por lapsos definidos, por ejemplo; sesiones interactivas periódicas de corta duración y para transmisiones de archivos en lote.

- Se debe limitar los tiempos de conexión al horario normal de oficina, puede existir un requerimiento operativo de extensión horaria.

21. Monitoreo del uso de los sistemas

21.1. Procedimientos y áreas de riesgo

- Se deben establecer procedimientos para monitorear el uso de las instalaciones de procesamiento de la información. Dichos procedimientos deben garantizar que los usuarios solo estén desempeñando actividades que hayan sido autorizadas explícitamente.

- El nivel de monitoreo requerido para cada una las instalaciones debe determinarse mediante una evaluación exhaustiva de riesgos.

Ítems que se pueden suscitar por mal uso y/o negligencia en los SGDB:

a) acceso no autorizado, incluyendo detalles como:

   1) Fecha y hora de eventos clave

   2) Bases de datos y registros a los que se accede

   3) ID's de usuario

   4) Tipos de eventos sucedidos

c) Intentos de acceso no autorizado, como:

   1) Violaciones de la política de accesos y notificaciones para "gateways" de red y "firewalls"

   2) Intentos fallidos

   3) Alertas de sistemas patentados para detención de intrusiones

b) Todas las operaciones con privilegio, como:

   1) Inicio y cierre (start-up and stop) del sistema

   2) Utilización de cuentas creadas

   3) Conexión y desconexión de dispositivos I/O

d) Alertas o fallas de sistema como:

   1) Alertas o mensajes de consola

   2) Excepciones del sistema de registro

   3) Alarmas del sistema de administración de redes

21.2. Factores de riesgo

- El resultado de las actividades de monitoreo se deben revisar periódicamente. Las revisiones dependerán de los riesgos involucrados.

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

- La experiencia acumulada en materia de infiltración y uso inadecuado de los SGDB y sus datos.
- La criticidad, la sensibilidad y el valor de la información contenida en las bases de datos involucradas;
- El alcance de la interconexión del sistema (en particular las redes públicas)
- La criticidad de los procesos de aplicaciones;

21.3. Registro y revisión de eventos

- Se debe considerar la posibilidad de copiar automáticamente los tipos de mensajes adecuados a un segundo registro, y/o utilizar herramientas de auditoría o utilitarios adecuados para llevar a cabo el examen de archivo.
- Se debe prestar especial atención a la seguridad de la herramienta de registro, debido a que si se accede a la misma en forma no autorizada, esto puede propiciar una falsa percepción de la seguridad.
- Una revisión de los registros debe incluir la comprensión de las amenazas que afronta el sistema y las maneras que surgen. Se podría requerir investigación adicional en caso de producirse incidentes relativos a la seguridad.
- En cuanto al monitoreo de seguridad se debe identificar eventos significativos ya que, los registros del SGDB contienen un gran volumen de información, gran parte de la cual es ajena al monitoreo de seguridad.

Asignar la responsabilidad por la revisión de registros, se debe considerar una reparación de funciones entre quien/es emprende/n la revisión y aquellos cuyas actividades están siendo monitoreadas.

Los controles deben apuntar a proteger contra cambios no autorizados y problemas operativos. Estos incluyen:

a) La desactivación de la herramienta de registro

b) Alteraciones a los tipos de mensajes registrados

c) Archivos de registro editados o suprimidos

d) Medio de soporte archivos de registro saturado, y falla en el registro de eventos o sobre escritura de los mismos.

21.4. Sincronización de relojes

La correcta configuración de los relojes de las computadoras es importante para garantizar la exactitud de los registros de auditoría, que pueden requerirse para investigaciones o como evidencia en casos legales o disciplinarios.

Los registros de auditorías inexactos podrían entorpecer tales investigaciones y dañar la credibilidad de la evidencia.

Cuando una computadora o dispositivo de comunicaciones tiene la capacidad de operar un reloj en tiempo real, este se debe configurar según un estándar acordado, por ejemplo. Tiempo Coordinado Universal (UCT) o tiempo estándar local. Como se sabe que algunos relojes se desajustan con el tiempo, debe existir un procedimiento que verifique y corrija cualquier variación significativa.

22. Computación móvil y trabajo remoto

Objetivo: Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remotas.

- La protección requerida debe ser proporcional a los riesgos que originan estas formas específicas de trabajo. Cuando se utiliza computación móvil deben tenerse en cuenta los riesgos que implica trabajar en un ambiente sin protección y se debe implementar la protección adecuada. En el caso del trabajo remoto la organización debe implementar la protección en el sitio de trabajo remoto ("teleworking site") y garantizar que se tomen las medidas adecuadas para este tipo de trabajo.

22.1. Computación móvil

- Se debe garantizar que la información de la empresa se comprometa mientras se esta utilizando dispositivos informáticos móviles, como por ejemplo; laptops, notebooks, palmtops, y teléfonos móviles,

- Se deben tomar recaudos al utilizar dispositivos informáticos móviles en lugares públicos, salas de reuniones y otras áreas no protegidas fuera de la sede de la organización. Se debe implementar protección para evitar el acceso no autorizado a la información almacenada y procesada por estas herramientas, o la divulgación de la misma, por ejemplo, mediante técnicas criptográficas. Es importante que cuando dichos dispositivos, son utilizados en lugares públicos se tomen recaudos para evitar el riesgo de que la información que aparece en pantalla, sea vista por personas no autorizadas. Se deben implementar procedimientos contra software malicioso y estos deben mantenerse actualizados. El equipamiento debe estar disponible para permitir un procedimiento de resguardo de la información rápido y fácil. Estos procedimientos deben estar adecuadamente protegidos contra, por ejemplo, robo o pérdida de la información. Se debe brindar protección adecuada para el uso de dispositivos móviles conectadas a redes. El acceso remoto a la información de la empresa a través de redes publicas, utilizando herramientas informáticas móviles, solo debe tener lugar después de una identificación y autenticación exitosas, y con mecanismos adecuados de control de acceso implementados.

- En ambientes no protegidos se debe adoptar una política formal que tome en cuenta los riesgos que implica trabajar con herramientas informáticas móviles. Por ejemplo, dicha política debe incluir los requerimientos de protección física, controles de acceso, técnicas criptográficas, resguardos y protección contra virus. Esta política también debe incluir reglas y asesoramiento en materia de conexión de dispositivos móviles a redes y orientación sobre uso de estos dispositivos en lugares públicos.

- Los dispositivos informáticas móviles también deben estar físicamente protegidas contra robo, especialmente cuando se dejan, por ejemplo, en automóviles y otros medios de transporte, habitaciones de hotel, centros de conferencias y ámbitos de reunión. El equipamiento que transporta información importante de la empresa, sensible y/o critica no debe dejarse desatendido y, cuando resulta posible, debe estar físicamente resguardado bajo llave, o deben utilizarse cerraduras especiales para asegurar el equipamiento.

- Se debe brindar entrenamiento al personal que utiliza computación móvil para incrementar su cocimiento de los riesgos adicionales ocasionados por esta forma de trabajo y de los controles que se deben implementar.

22.2. Trabajo remoto

- El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar fijo fuera de la organización.

- Se debe implementar la protección adecuada del sitio de trabajo remoto contra, por ejemplo; el robo de equipamiento e información, la divulgación no autorizada de información, el acceso remoto no autorizada a los sistemas internos de la organización o el uso inadecuado de los dispositivos e instalaciones. Es importante que el trabajo remoto sea autorizado y controlado por la gerencia, y que se implementen disposiciones y acuerdos para esta forma de trabajo.

- Las organizaciones sólo deben autorizar actividades de trabajo remoto si han comprobado satisfactoriamente que se han implementado disposiciones y controles adecuados en materia de seguridad y que estos cumplen con la política de seguridad de la organización.

- Las organizaciones deben considerar el desarrollo de una política, de procedimientos y de estándares para controlar las actividades de trabajo remoto.

  Se deben considerar los siguientes ítems:

  - La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local;

  - El ambiente de trabajo remoto propuesto;

  - Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que pasará a través del vinculo de comunicación y la sensibilidad del sistema interno;

  - La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo; familia y amigos.

22.3. Los controles y disposiciones comprenden:

- La provisión de mobiliario para almacenamiento y equipamiento, adecuado para las actividades de trabajo remoto.

- Una definición del trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar, los SGDB y servicios a los cuales el trabajador remoto esta autorizado a acceder.

- La provisión de un adecuado equipamiento de comunicación, con inclusión de métodos para asegurar el acceso remoto.

- Seguridad física

- Reglas y orientación para cuando familiares y visitantes accedan al equipamiento e información

- La provisión de hardware, soporte y mantenimiento del software
- Los procedimientos de back-up y para la continuidad de las operaciones
- Auditoría y monitoreo de la seguridad
- Anulación de la autoridad, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

23. Desarrollo y mantenimiento de sistemas

23.1. Requerimientos de seguridad de los sistemas

Objetivo: Garantizar que la seguridad sea incorporada a los sistemas de información.

- Antes del desarrollo de los sistemas de información, los requerimientos de seguridad deben ser identificados y aprobados ya que el diseño e implementación de los procesos comerciales que apoyen la aplicación o servicio pueden ser cruciales para la seguridad.

- En la fase de requerimientos de un proyecto, todos los requerimientos de seguridad incluyendo la necesidad de planes de reanudación, deben ser identificados, justificados, aprobados y documentados como un conjunto del caso de negocios de un sistema de información.

23.2. Especificaciones y análisis de los requerimientos de seguridad.

- Se deben especificar la necesidad de controles para las comunicaciones de requerimientos comerciales de sistemas nuevos o mejoras a los existentes. Éstas especificaciones deben considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo. Se deben realizar consideraciones afines al evaluar aplicaciones de bases de datos o paquetes de software para aplicaciones comerciales. Se considera adecuado que la administración de DB's utilice productos evaluados y certificados en forma independiente.

- Los requerimientos de seguridad y los controles deben reflejar el valor comercial de los recursos de información involucrados y el potencial daño al negocio que pudiere resultar por una falla o falta de seguridad. El marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan son la evaluación y la administración de riesgo.

- Los controles introducidos en la etapa de diseño de las aplicaciones deben ser significativamente más económicos para la organización para poder implementarlos y mantenerlos que aquellos controles incluidos durante o después de la implementación.

24. Seguridad en los sistemas de aplicación

Objetivo: Prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los SGDB.

- Se deben diseñar en los SGDB y en las aplicaciones utilizadas por los usuarios controles apropiados, pistas de auditoría o registros de actividad. Esto debe incluir la validación de datos de entrada, procesamiento interno y salida de datos.

- Pueden ser necesarios controles adicionales para los SGDB que procesan en recursos sensitivos, o tienen impacto valioso o críticos de la organización. Tales controles deben ser determinados sobre la base de requerimientos de seguridad y evaluación de riesgo.

24.1. Validación de datos de entrada

- Los datos de entrada en las bases de datos y sistemas de aplicación deben ser validados para asegurar que son correctos y apropiados.

- Los controles deben ser aplicados en los inicios de las transacciones, en datos permanentes (nombres y direcciones, límites de crédito, números de referencia al cliente) y tablas de parámetros (precios de venta, tasa de impuestos, índice de conversión de dinero), etc.

Deben considerarse los siguientes controles:

- Procedimientos para responder a errores de validación
- Procedimientos para determinar la verosimilitud de los datos
- Entrada dual u otros controles de entrada para detectar los siguientes errores:
  - Campos faltantes o incompletos
  - Caracteres inválidos en campos de datos
  - Controles de datos no autorizados o inconsistentes
  - Valores fuera de rango
  - Volúmenes de datos que exceden los limites inferior y superior
  - Revisión periódica de los contenidos de campos clave para confirmar su validez e integridad
  - Inspección de los documentos de entrada para detectar cambios no autorizados en los datos de entrada (todos los cambios a los documentos de entrada deben ser autorizados)
  - Determinación de las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

24.2. Controles de procesamiento interno

- Las actividades de procesamiento de datos debe ser supervisadas por el DBA o por la persona delegada por la gerencia de la empresa para estos menesteres.
- La confidencialidad de la información obtenida luego del procesamiento de datos debe ser protegida por el personal asignado a esta labor frente a terceros.

24.3. Áreas de riesgo

- Los controles de validación deben ser incorporados a los SGDB para detectar posibles alteraciones y/o corrupciones en los datos.
- El diseño de aplicaciones de bases de datos debe asegurar que las restricciones se implementen para minimizar los riesgos de fallas de procesamiento, conducentes a una pérdida de la integridad. Las áreas específicas a considerar incluyen:
  - El uso de software correcto para la óptima recuperación ante fallas, a fin de garantizar el correcto procesamiento correcto de los datos.
  - El uso y localización dentro de los programas, de funciones de suma y borrado para realizar cambios en los datos;
  - Los procedimientos para prevenir la ejecución de programas fuera de secuencia o cuando falló el procesamiento previo.

24.4. Controles y verificaciones

- Los controles requeridos dependerán de la naturaleza de la aplicación y de los eventuales impactos de posibles alteraciones de los datos ingresados a las bases de datos del negocio.

  Se pueden incluir los siguientes controles y verificaciones:

  - Validación de datos contenidos en el SGDB
  - Verificaciones de integridad de los datos, software bajado o cargado, entre computadoras centrales y remotas
  - Totales de control de registros y archivos de las DB's
  - Controles de sesión, para contrastar archivos de datos después de realizar actualizaciones de transacciones;
  - Controles de balance, para comparar balances de apertura con balances de cierre anteriores, por ejemplo:

- controles programa a programa
- controles ejecución a ejecución
- totales de actualización de archivos

- Comprobaciones para garantizar que los programas se ejecutan en el orden correcto y terminan en caso de producirse una falla, y que se detiene todo procesamiento posterior hasta que se resuelva el problema.

24.5. Validación de los datos de salida

La salida de datos desde los SGDB debe ser validada para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias. Normalmente en los SGDB se desarrollan para llevar a cabo una validación, verificación y prueba apropiadas, para garantizar que la salida siempre será correcta.

La validación de salidas debe incluir:

- Control y conciliación de cuentas de usuarios para asegurar el procesamiento de todos los datos
- Establecimiento de procedimientos para responder a las pruebas de validación de salidas
- Comprobaciones de la razonabilidad para verificar si los datos de salida son fidedignos y confiables
- Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente, determine la exactitud, totalidad, precisión y clasificación de la información;
- Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos

24.6. Desarrollo externo de software

Si se terceriza el desarrollo de software, se deben establecer los siguientes puntos:

- Acuerdos de licencias, derechos de propiedad intelectual y propiedad de códigos requerimientos contractuales con respecto a la calidad del código
- Certificación de la calidad y precisión del trabajo llevado a cabo
- Acuerdos de custodia en caso de quiebra de la tercera parte
- Derechos de acceso a una auditoría de la calidad y precisión del trabajo realizado
- Realización de pruebas previas a la instalación para detectar códigos troyanos.
- Se debe asegurar, garantizar y certificar la calidad en el desarrollo de los sistemas de aplicación.

25. Administración de la continuidad de los negocios

Objetivo: Neutralizar las interrupciones de las actividades comerciales y proteger los procesos de los SGDB críticos de los negocios de las derivaciones de fallas significativas o desastres.

- Se debe implementar un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad en los SGDB, mismos que podrían ocurrir por ejemplo; fallas en el equipamiento, accidentes, desastres naturales y/o acciones deliberadas

- Se deben analizar y gestionar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio de las bases de datos de la organización

- Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de los SGDB puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en validez y convertirse en una parte integral del resto de los procesos de administración y gestión.

- La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

25.1. Proceso de administración de la continuidad de los negocios

En la organización, se debe implantar un proceso controlado para el desarrollo y mantenimiento de la continuidad de los negocios.

Éste debe incluir los siguientes aspectos de la administración de la continuidad:

- Comprensión de los riesgos que enfrenta la organización en términos de probabilidad de ocurrencia e impacto, incluyendo la identificación y priorización de los procesos críticos de los negocios

- Elaboración y documentación de una estrategia de continuidad de los negocios consecuente con los objetivos y prioridades de los negocios acordados

- Elaboración y documentación de planes de continuidad del negocio de conformidad con la estrategia de continuidad acordada

- Pruebas y actualización periódicas de los planes y procesos implementados

- Comprensión del impacto que una interrupción puede tener en los negocios (es importante que se encuentren soluciones para los incidentes menos significativos, así como para los incidentes graves que podrían amenazar la viabilidad de la organización) y definición de los objetivos comerciales de las herramientas de procesamiento de información

- Garantizar que la administración de la continuidad de los negocios esté incorporada a los procesos y estructura de la organización. La responsabilidad por la

coordinación del proceso de administración de la continuidad debe ser asignada a un nivel jerárquico adecuado dentro de la organización, por ejemplo; al foro de seguridad de la información.

- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad del negocio

25.2. Continuidad del negocio y análisis del impacto

- La gerencia debe aprobar el desarrollo de un Plan Estratégico que determine el enfoque global con el que se abordará la continuidad de los negocios.

- Los eventos que causen interrupciones como por ejemplo; por fallas en el equipamiento, inundaciones e incendios deben ser identificados, luego llevar a cabo una evaluación de riesgos y así determinar el impacto que podrían tener estas interrupciones (tanto en términos de magnitud de daño como del período de recuperación). Estas dos actividades deben llevarse a cabo con la activa participación de los propietarios de los procesos y recursos de negocio. Esta evaluación considera todos los procesos de negocio y no se limita a las instalaciones de procesamiento de la información.

25.3. Elaboración e implementación de planes de continuidad de los negocios

Los planes deben ser desarrollados para mantener o restablecer las operaciones de los negocios en los plazos requeridos una vez ocurrida una interrupción o falla en los procesos críticos de los negocios.

En éste se deben considerar los siguientes puntos:

a) Identificar y establecer acuerdos con respecto a todas las responsabilidades y procedimientos de emergencia de la organización

b) Instrucción adecuada del personal en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis

c) Documentar los procedimientos y procesos acordados

d) Realizar pruebas y actualizaciones de los planes

e) Se debe asignar especial atención a la evaluación de dependencias en negocios externos y a los contratos vigentes; implementación de procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos.

- El proceso de planificación debe concentrarse en los objetivos de negocio requeridos, por ejemplo; restablecimiento de los servicios a clientes en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia ("fallback") en sitios alternativos de procesamiento de la información.

25.4. Marco para la planificación de la continuidad de los negocios

- Se debe mantener un solo marco para los planes de continuidad de los negocios, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

- Cada plan de continuidad debe especificar claramente las condiciones para su puesta en marcha, así como las personas responsables de ejecutar cada componente del mismo.

- Deben modificarse de conformidad con los procedimientos de emergencia establecidos, si se identifican nuevos requerimientos, por ejemplo; los planes de evacuación o los recursos de emergencia ("fallback") existentes.

Se deben tener en cuenta los siguientes puntos:

a) Cuando ha ocurrido un incidente se deben describir las acciones a realizar para evitar que se ponga en peligro las operaciones de la empresa y/o la vida humana. Se debe mantener contacto y buenas relaciones públicas pertinentes, por ejemplo; policía, bomberos y autoridades locales

b) Procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de las bases de datos de la organización

c) Las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos

d) Procedimientos de emergencia ("fallback") que describan las acciones a emprender para el traslado de actividades esenciales de la empresa o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos de negocio en los plazos requeridos

e) Un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo

f) Actividades de concientización e instrucción que estén diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces

g) Las responsabilidades de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan. Se deben mencionar alternativas cuando corresponda.

Cada plan debe tener un propietario específico. Los procedimientos de emergencia, los planes de reanudación ("fallback") y los planes de recuperación deben contarse entre las responsabilidades de los propietarios de los recursos o procesos de negocio pertinentes. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

25.5. Prueba, mantenimiento y reevaluación de los planes de continuidad de los negocios

- Los planes de continuidad deben ser probados periódicamente para garantizar que están actualizados y son eficaces, estas pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes.

- El cronograma de pruebas para los planes de continuidad del negocio debe indicar cómo y cuándo debe probarse cada elemento del plan. Se recomienda probar con frecuencia cada uno de los componentes del plan. Se deben utilizar diversas técnicas para garantizar que los planes funcionarán en la vida real.

  Las pruebas de los planes de continuidad deben incluir:

  - Pruebas de recuperación (garantizando que los SGDB y los sistemas de información puedan ser restablecidos con eficacia)
  - Pruebas de recuperación en un sitio alternativo (ejecutando procesos de negocio en paralelo, con operaciones de recuperación fuera del sitio principal)
  - Pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación del negocio utilizando ejemplo de interrupciones)
  - Simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis)
  - Pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído)
  - Ensayos completos (probando que la organización, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones)

Estas técnicas pueden ser utilizadas por cualquier organización y deben reflejar la naturaleza del plan de recuperación pertinente.

25.6. Mantenimiento y reevaluación del plan

- Deben mantenerse revisiones y actualizaciones periódicas de los planes de continuidad de los negocios para garantizar su eficacia permanente. Y en el programa de administración de cambios de la organización se deben incluir procedimientos para garantizar que se emprendan adecuadamente los tópicos de continuidad del negocio.

- Las revisiones periódicas de cada uno de los planes de continuidad del negocio se deben realizar asignando responsabilidades para cada revisión en cada uno de los planes. La identificación de cambios en las disposiciones relativas al negocio aún no reflejadas en los planes de continuidad debe seguirse de una adecuada actualización del plan. Este proceso formal de control de cambios debe garantizar que se distribuyan los planes actualizados y que se imponga el cumplimiento de los mismos mediante revisiones periódicas de todos los planes.

- "Entre los ejemplos de situaciones que podrían demandar la actualización de los planes se encuentra la adquisición de nuevo equipamiento, o la actualización ("upgrading") de los sistemas operacionales y los cambios de:
- Procesos, nuevos o eliminados
- Estrategia de los negocios
- Ubicación, instalaciones y recursos
- Personal
- Direcciones o números telefónicos
- Riesgos (operacionales y financieros)
- Legislación;
- Contratistas, proveedores y clientes clave".[1]

26. Cumplimiento de requisitos legales

Objetivo: Impedir infracciones, violaciones de las leyes del derecho civil y penal de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos y de los requisitos de seguridad.

- El diseño, uso, operación, administración de los SGDB deben estar circunscritos y sujetos a requisitos de seguridad legal, normativa y contractual.

- Se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados.

26.1. Identificación de la legislación aplicable

- Se deben definir y documentar formalmente todos los requisitos legales, normativos y contractuales pertinentes para cada SGDB, así como los controles específicos y las responsabilidades individuales para cumplir con dichos requisitos.

26.2. Derecho de propiedad intelectual del software

- El software propiedad de la empresa debe proveerse bajo acuerdo de licencia que limita el uso de los productos a máquinas específicas y puede limitar la copia a la obtención de resguardo solamente.

  Se deben considerar los siguientes controles:

  - Cumplimiento de condiciones y términos a cerca de la obtención de software e información en redes públicas.

  - Mantenimiento de pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

  - Creación de estándares y procedimientos formales para la adquisición de productos de software

  - Correcta conservación y un adecuado mantenimiento de los registros de la base de datos.

  - Implementación de controles que aseguren que no se exceda el máximo número permitido de usuarios de las DB's.

  - Realización de comprobaciones y verificaciones de que sólo se instalan productos de software autorizado y con licencia.

  - Dar cumplimiento del derecho de propiedad intelectual de software que defina el uso interno y legal de productos de información y de software desarrollado por la organización

  - Dar el mantenimiento y condiciones adecuadas con la utilización de licencias

  - Definir la normativa y procedimientos formales en cuento a la eliminación o transferencia de software a terceros.

- Poner en conocimiento de los usuarios el derecho de propiedad intelectual de software, las políticas de adquisición y notificación de la determinación de tomar acciones disciplinarias contra el personal que incurra en el cumplimiento de las mismas

- Selección y utilización de herramientas de auditoría adecuadas.

26.3. Reglas para la recolección de evidencia

- Se debe contar con adecuada y confiable evidencia para respaldar una acción en contra de una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria debe estar descrita en los procedimientos internos.

- Una evidencia que se presente debe cumplir con normas de evidencias establecidas en la ley pertinente o en las normas específicas cuando la acción implica la aplicación de una ley, tanto civil como penal.

Estas normas deben tener varias características:

a) Peso de la evidencia: la calidad y totalidad de la misma

b) Validez de la evidencia: si puede o no utilizarse la misma en un tribunal

c) Adecuada evidencia de que los controles aplicados en las bases de datos de la organización han funcionado en forma correcta y consistente (por ejemplo; evidencia de control de procesos) durante todo el período en que la evidencia a recuperar fue almacenada y procesada por el sistema.

26.4. Calidad y totalidad de la evidencia

- Para lograr una evidencia total y de calidad es necesaria la obtención de una sólida pista de la misma, para información en medios informáticos, así las pistas pueden establecerse si se cumplen las siguientes condiciones:

- Para documentos en papel: el original se almacena en forma segura y se mantienen registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo.

- Cuando se detecta un incidente puede no resultar obvio si éste derivará en una demanda legal. Por consiguiente, existe el riesgo de que la evidencia necesaria sea destruida accidentalmente antes de que se advierta la gravedad del incidente

- Se debe conservar un registro de todas las acciones realizadas durante el proceso de copia y éste debe ser presenciado. Se debe almacenar en forma segura una copia de los medios y del registro

- Para garantizar la disponibilidad de la información contenida en discos fijos, removibles, o en memoria, se deben realizar copias de la información en ellos contenida

- Cualquier investigación debe garantizar que la evidencia original no sea alterada

- En las primeras instancias de cualquier acción legal contemplada se debe procurar el asesoramiento por parte de un abogado y también es aconsejable involucrar a la policía.

26.5. Validez de la evidencia

- Para lograr que la evidencia tenga validez, las organizaciones deben asegurar que sus SGDB y sus sistemas de información cumplan con los estándares o códigos de práctica relativos a la producción de evidencia válida.

27. Compatibilidad técnica y revisiones de la política de seguridad

Objetivo: Garantizar la coincidencia de los SGDB con las normas, estándares y políticas de seguridad de la organización.

- La seguridad de los SGDB y de los sistemas de información debe revisarse periódicamente, dichas revisiones deben llevarse a cabo con referencia a las políticas de seguridad pertinentes.

- Las plataformas técnicas de los SGDB y sistemas de información de la organización deben ser auditados para verificar su compatibilidad con los estándares (normas) de implementación de seguridad.

27.1. Verificación de la compatibilidad técnica

- Se debe verificar periódicamente la compatibilidad de los sistemas de información con los estándares de implementación de la seguridad.

- La verificación de la compatibilidad técnica comprende la revisión de los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. Este tipo de verificación de cumplimiento requiere asistencia técnica especializada. Esta verificación debe ser realizada manualmente (de ser necesario, con el apoyo de adecuadas herramientas de software) por un ingeniero en sistemas experimentado, o por medio de software automatizado que genere un informe técnico para su ulterior interpretación por parte de un especialista.

- La verificación de compatibilidad también puede comprender pruebas de penetración, las cuales podrían ser realizadas por expertos independientes contratados específicamente con este propósito.

- Esto puede resultar útil para la detección de vulnerabilidades en el sistema y para verificar la eficacia de los controles con relación a la prevención de accesos no autorizados posibilitados por las mismas.

- Se deben tomar precauciones en caso de que una prueba de penetración exitosa pueda comprometer la seguridad del sistema e inadvertidamente permita explotar otras vulnerabilidades, las verificaciones de compatibilidad técnica sólo deben ser realizadas por personas competentes y autorizadas o bajo la supervisión de las mismas.

27.2. Cumplimiento de la política de seguridad

- La gerencia debe garantizar que se ejecuten correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. También, se debe tomar en cuenta la implementación de una revisión periódica de todas las áreas de la organización para garantizar el cumplimiento de los estándares y políticas de seguridad.

Las áreas a revisar son las siguientes:

a) usuarios

b) sistemas de información

c) gerentes.

d) proveedores de sistemas

e) propietarios de información y de recursos de información

- Los DBA y los usuarios de las bases de datos de la organización deben apoyar la revisión periódica de la conformidad de sus SGDB y sus sistemas de información con los estándares, políticas y otros requisitos de seguridad aplicables.

28. Argumentos de auditoría de sistemas

Objetivo: Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

- Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoría en el transcurso de las auditorías de sistemas. Asimismo, se requiere una protección adecuada para salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoría.

28.1. Protección de las herramientas de auditoría de sistemas

- Se debe proteger el acceso a las herramientas de auditoría de sistemas, por ejemplo; registros de bases de datos, campos, archivos de datos o software de auditoría; a fin de impedir compromiso o el mal uso de las mismas, éstas herramientas deben estar separadas de los sistemas operacionales, de desarrollo y no deben almacenarse en bibliotecas de cintas o en áreas de usuarios. Se debe otorgar un nivel adecuado de protección adicional.

28.2. Controles de auditoría de sistemas

- Los requerimientos y actividades de auditoría que involucran verificaciones de los sistemas operacionales deben ser cuidadosamente planificados y acordados a fin de minimizar el riesgo de discontinuidad de los procesos de negocio.

Se deben contemplar los siguientes puntos:

- Se debe convenir y controlar la eficacia de las verificaciones
- La solicitud y los requerimientos de auditoría deben ser acordados con la gerencia que corresponda
- Se deben identificar y convenir los requerimientos de procesamiento especial o adicional
- Se deben documentar de manera formal los procedimientos, requerimientos y responsabilidades
- Las actividades de auditoría deben estar limitadas a un acceso de sólo lectura del software de datos, el acceso que no sea de sólo lectura solamente debe permitirse para copias aisladas de archivos del sistema, las cuales deben ser eliminadas una vez finalizada la auditoría
- Se deben identificar claramente y poner a disposición los recursos de TI para llevar a cabo las verificaciones
- Todos los accesos deben ser monitoreados y registrados a fin de generar una pista de auditoría de referencia.

29. Recomendaciones

Entre las principales recomendaciones, se incluyen los siguientes grupos de políticas complementarias para la buena gestión de seguridad de la información, pues lo que se espera es que al ser colocadas en práctica se mejorar la seguridad de los ambientes informáticos de las Pymes.

29.1. Política de protección de oficinas, recintos e instalaciones

- Cuando no hay vigilancia, deben estar bloqueadas puertas y ventanas además debe considerarse la posibilidad de agregar protección externa a las ventanas, en particular las que se encuentran al nivel del suelo.

- Se deben implementar adecuados sistemas de detección de intrusos, estos deben ser instalados según estándares profesionales y deben ser probados periódicamente. Los sistemas abarcarán todas las puertas exteriores y ventanas accesibles.

- Los suministros a granel, como los útiles de escritorio, no deben ser almacenados en el área protegida hasta que sean requeridos.

29.2. Política de correo electrónico

- Debe contener básicamente los siguientes ítems:

  a) Se debe prevenir y asegurar la información de la organización de ataques al correo electrónico, por ejemplo; virus, interceptación

  b) Se debe dar protección de archivos adjuntos de correo electrónico, mediante encriptación si y sólo si la información a ser enviada requiere un elevado nivel de seguridad.

  c) Los lineamientos sobre cuando no utilizar correo electrónico deben estar claramente definidos, por ejemplo; no abrir correo de personas desconocidas, no abrir spams, no abrir archivos adjuntos.

  d) Se deben establecer responsabilidades del empleado para no comprometer a la organización, por ejemplo; enviando correos electrónicos difamatorios, llevando a cabo prácticas de hostigamiento, o realizando compras no autorizadas, para todas estas actividades se implementarán sanciones administrativas y controles disuasivos.

  e) Establecer para cuando sea necesario el uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos.

  f) Se debe retener los mensajes de correo electrónico, que podrían ser utilizados como pruebas en el ámbito jurídico o en casos de litigio.

  g) Se deben implementar controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

h) Establecer que el uso de correo electrónico de las organizaciones sólo tendrá el fin y uso "organizacional", quedando claro que no se permite el uso personal del mismo.

i) Se hará uso del correo electrónico de la forma más correcta posible, quedando prohibido; el envío y recepción de pornografía, correos personales, información empresarial no autorizada y otros que atenten contra el trabajo y fines empresariales.

30. Políticas del área de usuarios finales

30.1. Equipos desatendidos en áreas de usuarios

- Los usuarios finales de las bases de datos deben garantizar que los equipos desatendidos sean protegidos adecuadamente.

- Los equipos instalados en áreas de usuarios, por ejemplo; estaciones de trabajo o servidores de bases de datos, pueden requerir una protección específica contra accesos no autorizados, cuando se encuentran desatendidos durante lapso de tiempo extenso.

- Se debe concienciar a todos los usuarios, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus responsabilidades por la implementación de dicha protección.

Se debe comunicar a los usuarios de las bases de datos los siguientes puntos:

- Al finalizar las tareas concluir las sesiones activas deben protegerse las PC's mediante un mecanismo de bloqueo adecuado, por ejemplo; un protector de pantallas protegido por contraseña;

- Se debe proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo; contraseña de acceso.

- Se debe realizar el procedimiento de salida normal en las bases de datos cuando finaliza la sesión (no solo apagar la PC o terminal).

- Se debe cerrar completamente la base de datos si se va a dejar desatendida la misma por una período medio o largo de tiempo.

30.2. Política de utilización de controles criptográficos.

- Deben utilizarse sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

- Deben utilizarse técnicas y sistemas criptográficos para evitar comprometer la información contenida en archivos adjuntos que se han de enviar mediante red interna y/o externa.

- El uso de controles criptográficos debe estar enmarcado dentro del enfoque gerencial de las organizaciones, además debe estar conformado de principios generales mediante los cuales se propenda a proteger la información de la organización.

- Se debe utilizar sistemas y técnicas criptográficas en la administración de claves y también en la recuperación de información cifrada en caso de compromiso, daño o pérdida de las claves.

- Se debe establecer formalmente funciones y responsabilidades en:

- La implementación de la política

- La administración de las claves

- Se debe determinar el nivel apropiado de protección criptográfica y para que casos se lo utilizará

- Se debe adoptar estándares para la eficaz implementación en toda la organización (que solución se aplica para cada uno de los procesos de negocio)

- Se debe realizar una evaluación que posteriormente determinará si un control criptográfico es adecuado, que tipo de control debe aplicarse y conque propósito, y los procesos de la empresa.

30.3. Políticas para Cifrado

El cifrado es una técnica criptográfica que puede utilizarse para proteger la confidencialidad de la información. Se lo debe utilizar para la protección de información sensible o critica.

Considerar los siguientes ítems:

- Se debe identificar el nivel requerido de protección tomando en cuenta el tipo y la calidad de los algoritmos de cifrado utilizados y la longitud de las claves criptográficas a utilizar.

- Se deben considerar las restricciones y las normas nacionales e internacionales que podrían aplicarse junto al uso de técnicas criptográficas, y las cuestiones relativas al flujo de información cifrada a través de las fronteras.

- Se deben tomar en cuenta los controles aplicables a la exportación e importación de tecnología criptográfica.

- Se debe procurar el asesoramiento especializado para identificar el nivel apropiado de protección, a fin de seleccionar productos adecuados que suministren la protección requerida, y la implementación de un sistema seguro de administración de claves.

- Necesariamente en las organizaciones se debe contar con asesoramiento jurídico respecto a las leyes y normas que podrían aplicarse al uso del cifrado.

31. Políticas de Administración de claves criptográficas

31.1. Protección de claves criptográficas

- Debe ser esencial la administración de claves criptográficas para el uso eficaz de sistemas y técnicas criptográficas.

- Cualquier compromiso o pérdida de claves criptográficas puede conducir a un compromiso de la confidencialidad, autenticidad y/o integridad de la información.

- Se debe implementar un sistema de administración para respaldar el uso por parte de la organización, de los dos tipos de técnicas criptográficas, los cuales son:

  a) ***Técnicas de clave secreta,*** cuando dos o más actores comparten la misma clave y esta se utiliza tanto para cifrar información como para descifrarla. Esta clave tiene que mantenerse en secreto dado que una persona que tenga acceso a la misma podrá descifrar toda la información cifrada con dicha clave, o introducir información no autorizada;

  b) ***Técnicas de clave publica,*** cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) y una clave privada (que debe mantenerse en secreto). Las técnicas de clave pública pueden utilizarse para el cifrado y para generar firmas digitales.

     - Todas las claves deben ser protegidas contra modificación y destrucción, y las claves secretas y privadas necesitan protección contra divulgación no autorizada.

     - "Las técnicas criptográficas también pueden aplicarse con este propósito. Se debe proveer de protección física al equipamiento utilizado para generar, almacenar y archivar claves". [1]

31.2. Políticas del Sistema de administración de claves criptográficas

- Un sistema de administración de claves criptográficas debe estar basado en un conjunto acordado de normas, procedimientos y métodos seguros para:

  a) Cambiar o actualizar claves incluyendo reglas sobre cuando y como deben cambiarse las claves

  b) Recuperar claves comprometidas o perdidas como parte de la administración de la continuidad del negocio, por ejemplo; la recuperación de la información cifrada

  c) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones relacionadas con DB's.

  d) Revocar claves incluyendo como deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula de la organización (en cuyo caso las claves también deben archivarse)

e) Distribuir claves a los usuarios que corresponda, incluyendo como deben activarse las claves cuando se reciben

f) Ocuparse de las claves comprometidas

g) Generar y obtener certificados de clave pública

h) Archivar claves, por ejemplo; para la información archivada o resguardada

i) Destruir claves

j) Almacenar claves, incluyendo como obtienen acceso a las claves los usuarios autorizados

k) Registrar (logging) y auditar las actividades relativas a la administración de claves.

- Las claves asignadas a usuarios deben tener fechas de inicio de vigencia y de fin de vigencia, y serán utilizadas por un período limitado de tiempo, a fin de reducir su probabilidad de compromiso. Este período debe fijarse según se perciba el riesgo y las situaciones bajo las que se aplica el control criptográfico.

- Podría resultar necesario considerar procedimientos para administrar requerimientos legales de acceso a claves criptográficas, por ejemplo; puede resultar necesario poner a disposición la información cifrada en una forma clara, como evidencia en un caso judicial.

31.3. Políticas para la seguridad de los archivos del sistema

- Se debe controlar el acceso a los registros del SGDB.

- El mantenimiento de la integridad de la información contenida en el SGDB debe ser responsabilidad de la función usuaria o grupo de desarrollo a quien pertenecen los datos que entran a las bases de la organización.

31.4. Control del software operativo

A fin de minimizar el riesgo de alteración de los sistemas operacionales se deben tener en cuenta los siguientes controles:

a) La gerencia debe autorizar la actualización de las bibliotecas de programas operativos, la que sólo debe ser realizada por el cintotecario designado

b) Las versiones previas de software deben ser retenidas como medida de contingencia

c) Los sistemas en operación sólo deben guardar el código ejecutable si es posible

d) Las actualizaciones a las bibliotecas de programas operativos, se las debe mantener un registro de auditoría

e) Mientras no se haya actualizado las bibliotecas de programas fuente, pruebas y aceptación de usuario, el código ejecutable no debe ser implementado en un sistema operacional hasta tanto no se obtenga evidencia del éxito.

Además se debe considerar:

- Solo debe otorgarse acceso lógico o físico a los proveedores con fines de soporte y si resulta necesario, y previa aprobación de la gerencia. Las actividades del proveedor deben ser monitoreadas.

- Los parches de software sólo deben realizarse cuando puedan contribuir a mitigar las debilidades en materia de seguridad.

- Cualquier decisión referida a una actualización a una nueva versión debe tomar en cuenta la seguridad, por ejemplo; la introducción de una nueva funcionalidad de seguridad o el número y la gravedad de los problemas de seguridad que afecten esa versión.

- El mantenimiento del software suministrado por el proveedor y utilizado en los sistemas operacionales debe contar con el soporte del mismo.

31.5. Políticas de protección de los datos de prueba del sistema

- Los datos de prueba de las bases de datos deben ser protegidos y controlados.

- Las pruebas de aceptación de aplicaciones y sistemas normalmente requieren volúmenes considerables de datos de prueba, estos deben ser lo más cercanos como sea posible a los datos operativos.

- Se debe evitar el uso de bases de datos operativas que contengan información personal. Si se utiliza información de esta índole, esta debe ser despersonalizada antes del uso.

Cuando los datos operativos se utilizan con propósitos de prueba se deben aplicar los siguientes controles para proteger los datos:

a) La información operativa de un sistema de aplicación de prueba debe ser borrada inmediatamente después de completada la misma.

b) También se deben aplicar a los sistemas de aplicación de prueba así como procedimientos de control de accesos que se aplican a los sistemas de aplicación en operación.

c) Se debe suministrar pistas de auditoría mediante la copia y el uso de información operacional que deben ser registrado.

d) Se debe llevar a cabo una autorización por separado cada vez que se copia información operativa a un sistema de aplicación de pruebas de las bases de datos.

31.6. Control de acceso a las bibliotecas de programa fuente

- Mediante controles estrictos de acceso a las bibliotecas de programas fuente se debe minimizar la probabilidad de alteración de los programas de computadora, también se debe salvaguardar el acceso no autorizado a bibliotecas de programas fuente. Según los siguientes puntos:

a) Se debe designar a un cintotecario de programas para cada aplicación

b) Los listados de programas deben ser almacenados en un sitio (ambiente) seguro

c) El personal de soporte de TI debe tener acceso limitado a las bibliotecas de programas fuente

d) Las bibliotecas de programas fuente no deben ser almacenadas en los sistemas que están en producción

e) No deben ser almacenados en las bibliotecas de programas fuente operativos los programas en desarrollo o mantenimiento

f) El gerente de soporte de TI para la aplicación pertinente debe autorizar la actualización de bibliotecas de programas fuente y su distribución a los programadores, y ésta sólo solo debe ser realizada por el bibliotecario designado

g) El mantenimiento y la copia de las bibliotecas de programas fuente deben estar sujeta a procedimientos estrictos de control de cambios.

h) Las viejas versiones de los programas fuente deben ser archivadas con una clara indicación de las fechas y horas precisas en las cuales estaban en operación, junto con todo el software de soporte, el control de tareas, las definiciones de datos y los procedimientos

i) Se debe mantener un registro de auditoría de todos los accesos a las bibliotecas de programa fuente.

32. Políticas de seguridad de los procesos de desarrollo y soporte

Objetivo: Mantener la seguridad del software y la información del sistema de aplicación.

- Los gerentes deben garantizar que todos los cambios propuestos para el sistema sean revisados, a fin de comprobar que los mismos no comprometen la seguridad del sistema o del ambiente operativo.

- Los gerentes deben asignar se lleve a cabo el control estricto de los entornos de proyectos y el soporte a los mismos.

- Los gerentes responsables de los sistemas de aplicación también deben ser responsables de la seguridad del ambiente del proyecto y del soporte.

32.1. Políticas de procedimientos de control de cambios

Con la finalidad de reducir la posibilidad de alteración de los sistemas de información:

- Debe existir un control estricto de la implementación de los cambios

- Se debe imponer el cumplimiento de los procedimientos formales diseñados para el control de cambios.

- El control de cambios debe garantizar que no se comprometan los procedimientos de seguridad y control, los programadores de soporte deben tener acceso limitado, dándoles el debido acceso solamente a aquellas partes necesarias para el desempeño de sus tareas, éste acceso debe ser aprobado mediante acuerdos y asignaciones formales.

- Los cambios en el software de aplicaciones pueden tener repercusiones en el ambiente operativo. Siempre que resulte factible, los procedimientos de control de cambios operativos y de aplicaciones deben estar integrados.

- Estos procedimientos deben incluir el:

- Conservar un control de versiones para todas las actualizaciones de software

- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios

- Garantizar que los cambios son propuestos por usuarios autorizados

- Garantizar que el usuario autorizado acepte los cambios antes de cualquier implementación

- Garantizar que la implementación se lleve a cabo minimizando la discontinuidad de las actividades de la empresa

- Obtener aprobación formal para las propuestas detalladas antes de que comiencen las tareas

- Mantener un registro de los niveles de autorización acordados
- Mantener una pista de auditoría de todas las solicitudes de cambios
- Identificar todo el software, la información, las entidades de bases de datos y el hardware que requieran correcciones
- Garantizar que la documentación del sistema será actualizada cada vez que se completa un cambio y se archiva o elimina la documentación vieja
- Garantizar que la documentación operativa y los procedimientos de usuarios se modifiquen según las necesidades de adecuación
- Garantizar que la implementación de cambios tenga lugar en el momento adecuado y no altere los procesos comerciales involucrados.
- Es recomendable que se deban mantener en las organizaciones ambientes separados para; prueba del nuevo software por parte del usuario, para desarrollo y producción. Esto proporciona un medio para controlar el nuevo software y permitir la protección adicional de la información operacional que se utiliza con propósitos de prueba.

32.2. Políticas para la revisión técnica de los cambios en el sistema operativo

- Cuando la necesidad sea justificada y sólo cuando sea estrictamente necesario se debe cambiar el S.O.
- Se debe mantener constantemente actualizado el S.O., mediante parches de las versiones correspondientes.
- Cuando se realizan los cambios, se debe verificar y certificar la calidad de los sistemas de información los sistemas de aplicación deben ser revisados y probados para garantizar que no se produzca un impacto adverso en las operaciones o en la seguridad.

Este proceso debe cubrir el garantizar:

a) Que los procedimientos de integridad y control de aplicaciones no hayan sido comprometidos por los cambios del sistema operativo

b) Que el presupuesto y el plan de soporte anual contemple las revisiones y las pruebas del sistema que deban realizarse como consecuencia del cambio en el sistema operativo

c) Que se notifiquen los cambios del sistema operativo de manera oportuna antes de la implementación

d) Que se realicen cambios apropiados en los planes de continuidad de la empresa.

32.3. Políticas de restricción del cambio en los paquetes de software

- Siendo viable y en la medida de lo posible, los paquetes de software suministrados por proveedores deben ser utilizados sin modificación. Se debe desalentar la realización de modificaciones a los paquetes de software.

Cuando se considere esencial modificar un paquete de software, se deben tener en cuenta los siguientes puntos:

a) Previa cualquier modificación se debe obtener el consentimiento del proveedor;

b) Se debe tener en cuenta el riesgo de compromiso de los procesos de integridad y controles incorporados;

c) La posibilidad de obtener del proveedor los cambios requeridos como actualizaciones estándar de programas;

d) El impacto que se produciría si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

- Todos los cambios deben ser probados y documentados exhaustivamente, de manera que pueden aplicarse nuevamente, de ser necesario, a futuras actualizaciones de software.

- Si los cambios se consideran esenciales, se debe retener el software original y aplicar los cambios a una copia claramente identificada.

32.4. Políticas de seguridad frente al acceso físico por parte de terceros

Estas políticas tienen que ver con terceras partes y es necesario establecer la forma como se van a conducir las empresas frente a ellos, las políticas aquí propuestas quedan a elección de cada empresa para ser adoptadas según la necesidad de cada una de ellas.

- El acceso físico a las instalaciones de procesamiento de información de la organización por parte de terceros debe ser controlado.

- Los controles deben ser acordados y definidos en un contrato formal con la tercera parte.

- Dada la necesidad de la organización para permitir dicho acceso, debe realizarse una evaluación de riesgos para determinar posibles incidentes en la seguridad y los requerimientos de control.

- El acceso de terceros también puede involucrar otros participantes. Los contratos que confieren acceso a terceros deben incluir un permiso para la designación de otros participantes capacitados y las condiciones para su acceso. Este estándar puede utilizarse como base para tales contratos y cuando se considere la tercerización del procesamiento de información.

32.5. Políticas para contratistas in situ

Las terceras partes que sean aceptadas en el sitio por un lapso de tiempo establecido según estipulación, también pueden ocasionar debilidades en materia de seguridad. Entre los ejemplos de terceras partes in situ se listan los siguientes:

a) Consultores

b) Limpieza, "catering", guardianía de seguridad y otros servicios de soporte tercerizados

c) Personal de mantenimiento / soporte de hardware y software

d) Pasantías de estudiantes y otras designaciones contingentes de corto plazo

Es primordial establecer qué controles son precisos para gestionar el acceso de terceras partes a la infraestructura de procesamiento de información, todos los requerimientos de seguridad que reflejan los controles internos o del acceso de terceros, estarán presentes en los contratos celebrados con los mismos.

32.6. Requerimientos de seguridad en contratos con terceros

- No se debe otorgar a terceros acceso a la información ni a las instalaciones de procesamiento de la misma hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones para la conexión o para el acceso.

- Las instrucciones que observan el acceso de terceros a las instalaciones de procesamiento de información de la organización deben estar instituidas en un contrato formal que contenga todos los requerimientos de seguridad, o haga referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y estándares (normas) de seguridad de la organización.

- El contrato debe garantizar que no surjan malentendidos entre la organización y el proveedor. Las organizaciones deben estar satisfechas con las garantías de su proveedor.

"Se deben considerar las siguientes cláusulas para su inclusión en el contrato:

a) La política general de seguridad de la información

b) La protección de activos, con inclusión de:

   1) Procedimientos de protección de los activos de la organización, incluyendo información y software

   2) Procedimientos para determinar si se han comprometido los activos, por ejemplo; debido a pérdida o modificación de datos

   3) Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato, o en un momento convenido durante la vigencia del mismo

4) Integridad y disponibilidad

5) Restricciones a la copia y divulgación de información

c) Una descripción de cada servicio del que podrá disponerse

d) El nivel de servicio al que se aspira y los niveles de servicio que se consideran inaceptables.

e) Disposición que contemple la transferencia de personal cuando corresponda

f) Las respectivas obligaciones de las partes con relación al acuerdo

g) Responsabilidades con respecto a asuntos legales, por ejemplo; legislación referida a protección de datos, especialmente teniendo en cuenta diferentes sistemas legales nacionales si el contrato contempla la cooperación con organizaciones de otros países. Por ejemplo, si existe una necesidad específica de confidencialidad de la información, podrían implementarse acuerdos de no-divulgación.

h) Derechos de propiedad intelectual y asignación de derecho de propiedad intelectual, y protección de trabajos realizados en colaboración

i) Acuerdos de control de accesos que contemplen:

1) Los métodos de acceso permitidos, y el control y uso de identificadores únicos como ID's y contraseñas de usuarios

2) Un proceso de autorización de acceso y privilegios de usuarios

3) Un requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

j) La definición de criterios de desempeño comprobables, y el monitoreo y presentación de informes respecto de los mismos;

k) El derecho a monitorear, y revocar (impedir), la actividad del usuario;

l) El derecho a auditar responsabilidades contractuales o a contratar a un tercero para la realización de dichas auditoríass;

m) El establecimiento de un proceso gradual para la resolución de problemas; también deben considerarse, si corresponde, disposiciones con relación a situaciones de contingencia;

n) Responsabilidades relativas a la instalación y el mantenimiento de hardware y software;

o) Una clara estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos;

p) Un proceso claro y detallado de administración de cambios;

q) Los controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos;

r) Los métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad;

s) Los controles que garanticen la protección contra software malicioso

t) Las disposiciones con respecto a elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad;

u) La relación entre proveedores y subcontratistas."[1]

32.7. Políticas para el desarrollo de tareas en áreas protegidas

- Se debe evitar el trabajo no controlado en las áreas protegidas tanto por razones de seguridad así como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.

- Las áreas protegidas evacuadas deben ser físicamente bloqueadas y periódicamente inspeccionadas.

- El personal del servicio de soporte externo debe tener acceso limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso debe ser otorgado solamente cuando sea necesario, debe ser autorizado y monitoreado. Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

- No debe permitirse el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de equipamiento que registre información a las áreas críticas de la organización a menos que su ingreso se autorice expresamente.

32.8. Separación entre instalaciones de desarrollo e instalaciones operativas

- Se deben definir y documentar de una manera muy formal las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

- De manera deseable se deben separar las instalaciones de desarrollo, prueba y operaciones para así lograr también la separación de los roles involucrados.

- Las actividades de desarrollo y prueba pueden ocasionar problemas graves, como la modificación no deseada de archivos o sistemas, o la rectificación no deseada de fallas de sistemas.

- Se debe considerar el nivel de separación que resulta necesario entre los ambientes operativos, de prueba y de desarrollo, a fin de prevenir problemas operativos.

- También se debe implementar una separación similar entre las funciones de desarrollo y prueba. En este caso, existe la necesidad de mantener un ambiente conocido y estable en el cual puedan llevarse a cabo pruebas significativas e impedirse accesos inadecuados y no autorizados por parte del personal de desarrollo.

- Si el personal de desarrollo y prueba tiene acceso al sistema que esta operativo y a su información, éste puede ser capaz de introducir líneas de códigos no autorizados o no probados, o alterar los datos de las operaciones. En algunos sistemas esta capacidad puede ser utilizada inadecuadamente para perpetrar fraude, o para introducir programas no probados o maliciosos. Estos programas pueden ocasionar graves problemas operativos. El personal de desarrollo y pruebas también plantea una amenaza a la confidencialidad de la información operativa.

- Las actividades de desarrollo y pruebas pueden producir cambios no planificados en el software y la información si los sistemas comparten el mismo ambiente informático.

- La separación entre las instalaciones de desarrollo, pruebas y operaciones es por tanto deseable, a fin de reducir el riesgo de cambios accidentales o accesos no autorizados al software operativo y a los datos del negocio.

Se deben tener en cuenta los siguientes controles.

a) El software en desarrollo y en operaciones debe en la medida de lo posible, ejecutarse en diferentes procesadores o en diferentes dominios o directorios.

b) Es necesario que las actividades de desarrollo y prueba estén separadas.

c) Cuando no es requerido, los compiladores, editores y otros utilitarios del sistema no deben ser accesibles desde los sistemas que están operativos.

d) El personal de desarrollo sólo debe tener acceso a las contraseñas operativas, porque allí están adecuadamente ubicados los controles de emisión de contraseñas para el apoyo de los sistemas que se encuentran operativos. Estos controles deben garantizar que dichas contraseñas se modifiquen una vez utilizadas.

e) A fin de reducir el riesgo de error, se deben utilizar diferentes procedimientos de conexión ("log-on") para sistemas en operación y prueba. Se debe alentar a los usuarios a utilizar diferentes contraseñas para estos sistemas, y los menús deben desplegar adecuados mensajes de identificación.

32.9. Políticas para la administración de instalaciones externas

- Cuando la organización utilizase a un contratista externo para la administración de las instalaciones de procesamiento de información hay que considerar que esto puede dar lugar a potenciales exposiciones al riesgo en materia de seguridad, como la posibilidad de compromiso, daño o pérdida de datos en la sede del contratista. Estos riesgos deben ser identificados con anticipación, y deben acordarse controles adecuados con el contratista e incluirse en el contrato para orientación con respecto a contratos con terceros que contemplan el acceso a instalaciones de la organización y contratos de tercerización. Se deben abordar, entre otras, las siguientes cuestiones específicas:

a) Identificar las aplicaciones sensibles o críticas que convienen retener en la organización.

b) Obtener la aprobación de los propietarios de aplicaciones comerciales.

c) Implicancias para la continuidad de los planes comerciales.

d) Estándares de seguridad a especificar, y el proceso de medición del cumplimiento.

e) Asignación de responsabilidades específicas y procedimientos para monitorear con eficacia todas las actividades de seguridad pertinentes.

f) Responsabilidades y procedimientos de comunicación y el manejo de incidentes relativos a la seguridad.

32.10. Eliminación de medios informáticos

- Los medios magnéticos de almacenamiento cuando ya no son necesarios almacenamiento, deben se destruidos y eliminados de modo seguro. Si estos no se eliminan cuidadosamente, la información sensible de la organización puede filtrarse a personas ajenas a la organización.

- Se deben instaurar procedimientos formales para la destrucción y eliminación segura de los medios informáticos, a fin de minimizar este riesgo.

Deben considerarse los siguientes controles:

a) Los medios que contienen información sensible deben ser almacenados y eliminados de manera segura, por ejemplo incinerándolos, utilizando software de eliminación segura de la información confidencial (software de borrado seguro), o si se prescinde de los medios indicados simplemente haciéndolos trizas.

b) La siguiente lista especifica los ítems que deberían precisar de eliminación segura:

   - Documentación del sistema
   - Listados de programas
   - Informes de salida
   - Documentos en papel
   - Voces u otras grabaciones
   - Papel carbónico
   - Datos de prueba
   - Cintas de impresora de un solo uso
   - Cintas magnéticas
   - Discos o casetes removibles
   - Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).

c) Dependiendo de la complejidad, puede resultar más factible disponer que todos los medios sean agrupados y eliminados de forma segura, antes que intentar separar los ítems sensibles.

d) Se puede optar por la contratación de empresas que ofrecen servicios de recolección y eliminación de papeles, equipos y medios. Para ello se debe seleccionar cuidadosamente a una empresa contratista apto con adecuados controles y experiencia.

e) Se debe registrar la eliminación de los ítems sensibles, a fin de mantener una pista de auditoría.

Al acumular medios para su eliminación, se debe considerar el efecto de acumulación, que puede ocasionar que una gran cantidad de información no clasificada se torne más sensible que una pequeña cantidad de información clasificada.

Referencias Bibliográficas

[1] Instituto Argentino de Normalización Esquema 1 de Norma IRAM-ISO IEC17799, disponible en:http://seguridad.mendoza.gov.ar/tetra/Norma%20ISO%2017799%20Castellano.doc [12-noviembre-2006]

[2] Disponible en:http://www.ildis.org.ec/amparo/amparocont.htm, [15-Noviembre-2006]

Manual de Procedimientos para bases de datos en PYMES

Autor: Edwin Patricio Márquez Cadena

Junio de 2007

Índice

Esquema de contenidos

Introducción

En esta sección, como producto de la identificación de los activos a proteger, de la identificación de amenazas a las que están expuestas las Pymes, y una vez realizado el respectivo análisis de riesgos, se elaboran procedimientos para dos áreas de gran importancia en la gestión de bases de datos en las Pymes, estas son: Administración de bases de datos y Fortalecimiento del sistema operativo, en estas áreas se detallan 13 procedimientos para la primara área y 9 para la segunda. Se sugiere a las Pymes tomar en cuenta y poner en práctica estos importantes procedimientos para la apropiada y segura gestión de las bases de datos de cada una de las empresas.

Objetivos

- Conseguir que las Pymes pongan en práctica estos procedimientos para la adecuada gestión y operación de las bases de datos en dichas empresas.

- Definir mediante los pasos específicos que se deben dar en cada procedimiento las actividades a realizar para llevar a cabo el mencionado procedimiento.

- Establecer estos procedimientos como un documento formalizado para la gestión de las bases de datos en Pymes.

Área 1: Administración de Base de Datos

PR01. Creación de la base de datos

Objetivo.- Definir los pasos necesarios para que el administrador de la base de datos realice la creación de una base de datos.

Procedimiento:

1. Determinar la unidad y directorio dónde se instalará el SGBD y la data de la base de datos, los cuales deberán ser diferentes.

2. Instalar el SGBD en el PC o servidor si es que aún no está instalado

3. Crear automáticamente la base de datos durante la instalación o manualmente posterior a la instalación, asignándole un nombre adecuado.

4. Especificar la o las claves para el usuario administrador de la base de datos.

5. Probar la conexión a la base de datos, mediante el cliente correspondiente.

PR02. Administración de cuentas de usuarios

Objetivo.- Definir los pasos necesarios para administrar y controlar la asignación, manejo y buen uso de las cuentas de usuario; así como sus perfiles y roles.

Procedimiento:

1. Definir los niveles de acceso para el usuario que se va ha crear.
2. Seleccionar/crear perfiles y roles de usuario
3. Crear/modificar usuario desde la consola de seguridad de la base de datos considerando las políticas establecidas para la generación de claves.
4. Asignar perfiles y roles a usuario.
5. Mantener los perfiles y roles asignados; a los usuarios y a esos perfiles, mediante las siguientes acciones:
   - Actualizar los niveles de acceso
   - Chequear la interoperabilidad con otras bases de datos
   - Controlar la periodicidad de los accesos
   - Planificar la calendarización de accesos.
   - Eliminar y/o modificar de cuentas de usuario que así lo requieran.

PR03. Integridad de los datos

Objetivo.- Garantizar la integridad de los datos almacenados en las bases de datos de la organización.

Procedimiento:

1. Definir los límites tanto para recursos generales como para los recursos de contraseñas.
2. Establecer controles de seguridad y recuperación
3. Establecer y analizar los controles de concurrencia
4. Establecer controles de vista
5. Establecer y mantener controles de acceso

PR04. Monitoreo de cuentas de usuario

Objetivo.- Controlar y verificar el uso adecuado de las cuentas de usuario de la base de datos.

Procedimiento:

1. Chequear el uso de cuentas; frecuencias de acceso y frecuencias de uso.
2. Monitorear los sitios dónde se originan las conexiones.
3. Testear accesos de usuarios / tiempo de conexión a la base de datos.
4. Definir el tiempo base para eliminación de cuentas que después de un tiempo limitado no se hayan conectado a las bases de datos.
5. Decidir el tiempo en el cual se caducan las cuentas y passwords.
6. Ejecutar el análisis de cuentas para detectar los accesos no autorizados.

PR05. Pruebas de control operacional

Objetivo.- Identificar y establecer las distintas pruebas que se deben realizar para mantener bases de datos en un nivel óptimo y operativo.

Procedimiento:

1. Verificar qué datos están siendo usados, quién esta usando el sistema de base de datos, y durante que tiempo serán utilizados.
2. Realizar seguimientos de ejecución a las consultas.
3. Verificar posibles cuellos de botella, qué recursos de hardware están siendo usados por el sistema de base de datos, cuándo son usados.
4. Analizar tiempos de espera para la ejecución de consultas y programas
5. Verificar cuánto tiempo se usa por una rutina de procesamiento en comparación con una consulta ad hoc.
6. Realizar estadísticas de los datos de entrada y salida.

PR06. Cargas en Bases de Datos

Objetivo.- Proporcionar los pasos necesarios para realizar carga de datos en una nueva base de datos o un SGDB, ofreciendo datos íntegros para su uso.

Procedimiento:

1. Seleccionar, depurar y transformar los datos desde la fuente original de datos.

2. Validar los datos; crear script de exportación, ejecutarlo y revisar el log generado para determinar que no existan errores.

3. De existir errores en el log generado; corregirlos y ejecutarlo nuevamente.

4. Importar los datos a la base de datos destino, revisar el log generado de la importación para determinar que no hay errores.

5. Asignar los permisos necesarios a los usuarios o esquemas que lo requieran.

PR07. Mantenimiento en Bases de Datos

Objetivo.- Definir los pasos para realizar el mantenimiento periódico del SGDB para que los datos contenidos, estén disponibles permitiendo así la continuidad de las operaciones.

Procedimiento:

1. Chequear; buffers, índices, tablas y dispositivos de almacenamiento, para determinar su adecuación a medida que cambian los requisitos del sistema;

2. Verificar que estén activos y asignados los permisos correspondientes para realizar las operaciones de; insert, delete y update en las bases de datos para los usuarios que lo requieran.

3. Chequear el tamaño de las bases de datos, por su crecimiento dinámico.

4. Verificar las aplicaciones de la base de datos que pueden cambiar debido a nuevos requisitos.

5. En base a la información anterior tomar la decisión de adicionar o actualizar recursos y prever necesidades futuras.

PR08. Backup y recuperación

Objetivo- Definir los pasos necesarios para realizar copias de seguridad de manera que sea posible la completa recuperación de los datos.

Procedimiento:

1. Seleccionar la herramienta, tipo de respaldo y periodicidad para obtener los respaldos, además seleccionar el medio magnético de almacenamiento previo a la posterior recuperación completa de los datos.

2. Obtener copias de seguridad, ya sean de entorno global o de un esquema definido, se sugiere realizarlas de manera diaria.

3. Realizar copias de seguridad, de acuerdo a los tipos conocidos; completa, incremental, diferencial y de acuerdo a las estrategias de rotación; padre-hijo, abuelo-padre-hijo, torres de Hanoi.

4. Almacenar las copias de seguridad en sitios seguros, para facilitar la recuperación inmediata se sugiere tener la última copia de seguridad cerca del lugar de trabajo y la otra copia en otro edificio.

5. Verificar que la copia ha sido generada exitosamente, eligiendo una de las siguientes formas:

    a) Restaurar la copia en un entorno de prueba

    b) Revisar el log generado por la herramienta de generación de respaldos si ésta así lo permite, para detectar posibles errores o anomalías.

    c) Comparar el tamaño de la copia obtenida con el tamaño de la copia anterior, si ha aumentado está bien, pero si hay reducción en el tamaño puede haber ocurrido un error.

6. Realizar la recuperación a partir de la última copia de seguridad, si y solo si la esta copia de seguridad garantiza que los datos están completos.

7. Controlar que los datos son actuales y que no existan pérdidas de los mismos.

PR09. Administración de los cambios en el sistema de base de datos

Objetivo.- Definir los pasos necesarios para realizar cambios en la configuración o a las bases de datos de una manera adecuada, documentada y sobretodo segura.

Procedimiento:

1. Previo a la realización de cambios en la base de datos asegurar que se tiene una copia de seguridad del sistema actual.

2. Si se requiriere de cambios en el sistema de base de datos, supervisar las nuevas implantaciones con el objetivo de medir su impacto real.

3. Supervisar para predecir efectos de cambios necesarios a futuro.

4. Registrar los cambios realizados a la configuración o a la base de datos.

PR10: Monitoreo y Programación de Alarmas

Objetivo.- Mantener control sobre el desempeño del SGDB, para evitar en lo posible fallos de la Base de Datos.

Procedimiento:

1. Definir la alerta

2. Definir el grado de criticidad de la alerta

3. Definir los medios de aviso de la alerta, por; e-mail, mediante archivo de log, vía celular, aviso en la base de datos

4. Crear el Plan de Contingencias de la alerta

5. Resolver o gestionar la alerta

6. Registrar la alerta en la bitácora

7. Documentar la resolución de la evacuación.

PR11: Optimización de la base de datos

Objetivo.- Mantener puesto a punto el servidor de la base de datos, tanto a nivel de Arquitectura como a nivel de Memoria.

Procedimiento:

1. Elaborar planes de estadísticas
2. Verificar, calcular y evaluar las tendencias de crecimiento (esquemas, usuarios, información)
3. Chequear reportes de logs, estadísticas, (revisar y analizar la base de datos y el sistema operativo).
4. Elaborar el plan de afinamiento
5. Probar el plan de afinamiento (ambiente de pruebas)
6. Aplicar el plan de afinamiento de la base de datos
7. Monitoreo del rendimiento y la disponibilidad de servicio
8. Elaborar la bitácora.

PR12: Actualización de Versiones y Aplicación de Parches

Objetivo.- Mantener el servidor actualizado y al Software de base sin fallos.

Procedimiento:

1. Acceder a la Web, para descargar los parches y actualizaciones, dependiendo del tipo de base de datos actualizar. Para SQL Server, acceder a http://www.microsoft.com, buscar sus parches y descargarlos. En el caso de Oracle, se debe ingresar a Metalink o a http://otn.oracle.com y buscar los parches, descargarlos y seguir los pasos secuenciales indicados para actualizar o parchear.
2. Instalar los parches y actualizaciones en un servidor de pruebas que tenga la misma configuración de los servidores de producción.
3. Evaluar la consistencia de la base de datos después de la actualización.
4. De no existir problemas en el punto 3, aplicar las actualizaciones a los servidores de base de datos de producción.

PR13. Auditoría

Objetivo.- Configurar o aplicar auditoría, para garantizar que los objetos de las bases de datos contengan controles para verificar quien accede a que objeto, que cambios realiza y que operaciones ejecutó; y que estas operaciones están siendo registradas para realizar acciones de seguimiento y mezcla algunas opciones enfocadas a sistema operativo y otras a base de datos.

Procedimiento:

1. En caso de ser posible y necesario activar la auditoría de la base de datos aplicándolo a los eventos y objetos que requieran ser auditados.

2. Revisar los logs generados por el proceso activado.

3. Respaldar los logs o datos generados.

4. Proteger los registros de auditoría guardando sus registros fuera de la base de datos, en las pistas de auditoría dependiendo del sistema operativo.

Área 2: Fortalecimiento del sistema operativo

PR14: Actualizaciones de sistema operativo

Objetivo.- Definir los pasos necesarios para actualizar el sistema operativo con los parches de seguridad que se encuentren disponibles.

Procedimiento:

Se puede actualizar el sistema operativo mediante tres formas:

1. Desde el cliente de navegación: Internet Explorer, ir al menú Herramientas, hacer clic en Windows Update; revisar las actualizaciones disponibles para el equipo, seleccionar las que se deseen instalar finalmente instalarlas y reiniciar el equipo.

2. Configurar la herramienta Actualizaciones automáticas desde Panel de Control, pudiéndose elegir entre: Automático, en caso de que el equipo esté conectado a Internet, para que se descarguen las actualizaciones a cierta hora durante los días que se indiquen; Descargar actualizaciones manualmente, para usuarios con experiencia. Una de las dos formas es recomendable dejar activada. **1** Sugerida para Pequeñas Empresas, también para asegurarse de que no hay actualizaciones a ejecutar utilizar la forma **2**.

3. Instalar un servidor WSUS, y en cada cliente configurar para que las actualizaciones se realicen desde ese servidor; sugerido para Medianas empresas con posibilidad de poderlo implementar.

PR15: Eliminar servicios de Windows

Objetivo: Definir los pasos necesarios para eliminar los servicios, funcionalidades y protocolos innecesarios; para reducir la superficie de ataque.

Procedimiento:

1. Para cambiar la configuración por defecto de los servicios de Windows se debe cambiar el estado de un servicio, desde Inicio → todos los programas → herramientas administrativas → servicios, clic sobre el servicio deseado y seleccione pestaña general.

   a) Dependiendo del estado, podrá; iniciarlo, detenerlo, pausarlo o reanudarlo.

   b) Seleccione Manual, Automático o Deshabilitado.

2. Para cambiar la identidad con la que se ejecuta el servicio, seleccione iniciar sesión → cuenta del sistema local, si desea que se ejecute como (LocalSystem) o si desea que se ejecute como usuario seleccione la opción esta cuenta, rellenar las credenciales adecuadamente → Aceptar.

PR16: Administración de cuentas de Windows

Objetivo: Definir los pasos para administrar las cuentas de usuario **de Windows** mediante la activación y el uso de contraseñas.

Procedimiento:

1. Si se trata de nuevos usuarios activar la opción de crear contraseña.

2. Las cuentas de usuario que no se utilicen deben borrarse o desactivarse, tanto para PC's o grupos de trabajo:

   a) Escritorio → Mi PC, con el botón derecho seleccionar Administrar, seleccione administración del equipo (local) → herramientas del sistema → usuarios locales y grupos → usuarios.

   b) Para borrar una cuenta selecciónela y pulse Supr.

   c) Para desactivarla, haga doble clic sobre la cuenta y verifique la cuenta deshabilitada.

   d) Desactivar el modo de inicio de sesión con pantalla de bienvenida ya que informa a cualquier persona con acceso físico sobre los usuarios del equipo.

   e) Activar el protector de pantalla con contraseña:

      En cualquier parte del escritorio hacer clic, seleccione Propiedades → pestaña de protector de pantalla → seleccione cualquier protector → verificar la casilla Proteger con contraseña al reanudar.

PR17: Establecer directivas de contraseñas

Objetivo: Establecer directivas de contraseñas que permitan controlar la complejidad de contraseñas, el bloqueo de cuentas, la caducidad de contraseñas y el historial de contraseñas.

Procedimiento:

Estas restricciones se imponen en las contraseñas en Windows XP/2000/2003 por medio de directivas de seguridad.

1. Inicio → todos los programas → herramientas administrativas directiva de seguridad local. Desplegar Directivas de cuentas → directivas de contraseñas → (configurar complejidad de contraseñas, su caducidad, el historial).

2. Despliegue el nodo de directivas de cuenta → directivas de bloque de cuenta (umbral de bloques de cuenta, duración del bloqueo de cuenta).

3. Crear mensajes (disuasorios), de advertencia, para el cumplimiento de medidas de seguridad;

4. En la ventana Directiva de seguridad local → Directivas locales → Opciones de seguridad, localizar Inicio de sesión interactivo (escriba un texto para el título de la ventana que mostrará al usuario cada vez que inicie una sesión → localice Inicio de sesión interactivo (texto para los usuarios que intentan iniciar una sesión.

PR18: Configuración de cortafuegos de sistema operativo Windows XP/2000/2003

Objetivo: Definir los pasos necesarios para configurar de una manera segura el cortafuegos de Windows

Procedimiento:

La forma de configurarlo es la siguiente:

1. En el escritorio, sobre el icono Mis sitios de red, hacer clic con el botón secundario del mouse y seleccionar propiedades.

2. Haga clic sobre la conexión que desee proteger y pulse el botón propiedades

3. Haga doble clic sobre el protocolo de Internet (TCP/IP) y pulse el botón Avanzada

4. Seleccionar la pestaña opciones, hacer doble clic sobre filtrado TCP/IP

5. En puertos TCP, elegir la opción Permitir sólo Para cada número de puerto que se desee permitir, seleccione el botón Agregar y escríbalo.

PR19: Monitoreo de servidores

Objetivo: Definir los pasos para establecer un permanente control y monitoreo de los principales recursos que disponen los servidores.

Procedimiento:

1. Establecer conexión remota al servidor y visualizar que los recursos se encuentren operando de manera aceptable.

2. Revisar los siguientes parámetros configurados en el Monitor de aplicaciones

   - Cantidad de memoria utilizada/disponible.
   - Espacio disponible en disco.
   - Carga soportada por el procesador.
   - Interfaz de red paquetes recibidos y enviados
   - Conexiones remotas establecidas.
   - Permisos de los usuarios creados en el sistema operativo.

3. Ubicarse en el nombre de cada servidor listados en el Monitor y dentro de ellos revisar los resultados de cada parámetro establecido anteriormente.

PR20: Instalación de software antivirus

Objetivo: Mantener libre de virus los equipos y las redes de organización, para así garantizar su normal funcionamiento y la disponibilidad de la información contenida en las DB's y SI de la organización, también evitando su pérdida o daño, permitiendo así la continuidad de los negocios de la organización.

Procedimiento:

1. Elección e Instalación de la solución antivirus adecuada a la infraestructura y tamaño de la empresa.

2. Instalar antivirus perimetrales para empresas medianas, antes que alcancen la red interna; se suele combinar antivirus de diferentes compañías, es decir una marca para los dispositivos perimetrales, otra para los puestos de trabajo y una tercera marca para los servidores.

3. Instalar adicionalmente firewalls perimetrales en empresas que tienen implementada su red.

4. Instalar (IDS), sistemas de detección de intrusos.

5. Instalar soluciones antivirus en los servidores de DB's y aplicaciones.

6. Instalar herramientas de detección y eliminación de Spyware

7. En el caso de pequeñas empresas; instalar antivirus de equipos de sobremesa, además se sugiere la instalación de firewalls personales.

PR21: Ejecución de antivirus

Objetivo: Mantener libre de virus y operativos los equipos y redes de la organización, así como el software contenido en los mismos, permitiendo la continua disponibilidad de la información y la continuidad de los negocios.

Procedimiento:

1. Para ejecutar un antivirus primero debe estar configurado, así:
2. El funcionamiento debe configurarse como background, en tiempo real o autoprotección para monitorizar el sistema constantemente.
3. Habilitar el escaneo de memoria, los sectores de arranque y del sistema de archivos al inicio del sistema.
4. Ejecución manual en equipos de sobremesa.
5. Instalar dos antivirus de distintas marcas para lograr mayor seguridad antivirus.
6. Escaneo continuo de firewalls en la red empresarial, debe correr conjuntamente con el antivirus.
7. De preferencia se debe programar el administrador de tareas del sistema operativo para la ejecución automática del antivirus.

PR22: Actualización de antivirus

Objetivo: Mantener actualizado el software antivirus, así como la lista de definición de virus, protegiendo de una manera óptima los equipos y software en él instalados.

Procedimiento:

1. Actualizar el antivirus desde la página web del fabricante, de manera automática y de forma regular.
2. Actualizar de modo manual, su periodicidad; semanal.
3. Suscribirse a un servicio de alerta, y actualizarse cuando reciba esta.
4. Disponer de una consola centralizada por medio de la cual realizar actualizaciones y luego distribuirlas a los demás equipos. Determinar el nivel de funcionamiento de los antivirus en los equipos.