SEGURIDAD DE LAS OPERACIONES

Procedimientos y responsabilidades operacionales

Tiene como objetivo asegurarse de las operaciones correctas y seguras de los recursos de procesamiento de la información.

Procedimientos de operación documentados

Los procedimientos de operación deberían ser documentados y estar disponibles para todos los usuarios que los necesiten.

Deberían elaborarse procedimientos documentados para las actividades operacionales asociadas con los recursos de comunicaciones y de procesamiento de información, tales como procedimientos de arranque y apagado del computador, respaldo, mantenimiento de equipos, manejo de medios, gestión y seguridad de la sala de cómputo y la utilización de correo.

Los procedimientos operacionales deberían especificar las instrucciones de operación, incluyendo:

a) la instalación y configuración de los sistemas;

b) el procesamiento y manejo de la información, tanto automatizada como manual;

c) respaldo;

d) requisitos calendarizados, incluyendo interdependencias con otros sistemas, tiempos de comienzo y terminación de tareas, tempranas y tardías

e) instrucciones para el manejo de errores u otras condiciones excepcionales, que pudieran surgir durante la ejecución de la tarea, incluyendo restricciones en el uso de las utilidades de sistema;

f) soporte y contactos de escalamiento incluyendo contactos de soporte externo en caso de dificultades operacionales o técnicas inesperadas;

g) instrucciones para el manejo de medios y salidas especiales, tales como la utilización de papelería especial o la gestión de salidas confidenciales incluyendo los procedimientos para el desecho seguro de la salida de trabajos fallidos;

h) procedimientos de reinicio y recuperación del sistema para el uso en caso de falla;

i) la gestión de las pistas de auditoría y de la información de la bitácora del sistema;

j) procedimientos de supervisión.

Los procedimientos de operación y los procedimientos documentados para las actividades del sistema, deberían tratarse como documentos formales y que los cambios sean autorizados por la dirección. Cuando sea técnicamente posible, los sistemas de información deberían gestionarse de forma coherente, usando los mismos procedimientos, herramientas y utilidades.

SEGURIDAD DE LAS OPERACIONES

Gestión de cambios
Se deberían controlar los cambios de la organización, en los procesos de negocio, recursos de procesamiento de la organización y en los sistemas que afecten la seguridad de la información.

En particular deberían considerarse los siguientes elementos:

a) identificación y registro de cambios significativos;

b) planificación y pruebas de los cambios;

c) evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad de la información;

d) procedimiento formal de aprobación para los cambios propuestos;

e) verificación de que se han cumplido los requisitos de seguridad de la información;

f) comunicación de los detalles del cambio a todas las personas pertinentes;

g) procedimientos de reversión, incluyendo procedimientos y responsabilidades para abortar y recuperar los cambios sin éxito y de acontecimientos imprevistos.

h) provisión de un proceso de cambio de emergencia para permitir la implementación rápida y controlada de los cambios necesarios para resolver un incidente.

Deberían establecerse las responsabilidades y los procedimientos formales de gestión para asegurar el control satisfactorio de todos los cambios. Cuando se realizan los cambios, debería conservarse una bitácora de auditoría conteniendo toda la información pertinente.

El control inadecuado de cambios en los recursos y los sistemas de procesamiento de información es una causa común de las fallas del sistema o de la seguridad. Los cambios al ambiente de producción, especialmente al transferir un sistema del estado de desarrollo al de producción, pueden impactar la confiabilidad de las aplicaciones.

Gestión de la capacidad
El uso de los recursos debería ser supervisado, ajustado y basado en proyecciones de los futuros requisitos de capacidad para asegurar el rendimiento del sistema requerido.

Los requisitos de capacidad deberían ser identificados, tomando en cuenta la criticidad para el negocio del sistema en cuestión. El ajuste y seguimiento deberían ser aplicados al sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y la eficacia de los sistemas. Deberían ejecutarse controles de detección para indicar problemas a su debido tiempo. Las proyecciones de los requisitos de capacidad futura deberían tomar en cuenta los nuevos requisitos del negocio y del sistema, así como tendencias actuales y proyectadas en la capacidad de procesamiento de la información de la organización.

Es necesario poner atención a cualquier recurso cuya adquisición toma mucho tiempo o requiere costos elevados; por lo tanto, los administradores deberían supervisar la utilización de los recursos clave del sistema. Ellos deberían identificar tendencias en el uso, particularmente en lo referente a las aplicaciones del negocio o herramientas de gestión de sistemas de información.

Los administradores deberían utilizar esta información para identificar y evitar posibles cuellos de botella, así como dependencia de personal clave que pudiera presentar una amenaza a la seguridad del sistema o servicios, y planificar la acción apropiada.

El proveer capacidad suficiente puede ser logrado mediante el aumento de la capacidad o la reducción de la demanda. Algunos ejemplos de la gestión de la demanda de capacidad son:

a) la eliminación de datos obsoletos (espacio en disco)

b) el retiro de aplicaciones, sistemas, base de datos o ambientes;

c) la optimización de procesos por lotes y calendarización;

d) la optimización de la lógica de la aplicación o las consultas de la base de datos;

e) la denegación o restricción del ancho de banda para los servicios que demandan gran cantidad de recursos, si no son críticos para el negocio (por ejemplo, trasmisión de vídeos).

Debería considerarse un plan documentado de gestión de la capacidad para los sistemas de misión crítica.

Este control también se refiere a la capacidad de los recursos humanos, así como de las oficinas e instalaciones.

Separación de los ambientes para desarrollo, pruebas y producción
Los ambientes para desarrollo, pruebas y producción deberían estar separados para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.

Debería identificarse e implementarse el grado de separación entre los ambientes de desarrollo, prueba y producción que es necesario para prevenir problemas operacionales.

Los siguientes puntos deberían considerarse:

a) deberían definirse y documentarse las reglas para transferir el software del ambiente de desarrollo al de producción;

b) el software de desarrollo y el de producción deberían funcionar en sistemas y procesadores de computadores diferentes, y en dominios o directorios distintos;

c) los cambios en los sistemas y aplicaciones en producción deberían probarse en un ambiente de pruebas o ensayos, antes de ser aplicados a los sistemas en producción;

d) salvo en circunstancias excepcionales, las pruebas no deberían hacerse en los sistemas en producción;

e) los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas en producción, cuando no sea requerido;

f) los usuarios deberían emplear perfiles de usuario diferentes para los sistemas en producción y pruebas y los menús deberían desplegar los mensajes de identificación apropiados para reducir el riesgo a errores;

g) los datos sensibles no deberían copiarse en el ambiente del sistema de prueba, a menos que se proporcionen controles equivalentes para el sistema de prueba.

Las actividades de desarrollo y prueba pueden causar serios problemas, por ejemplo, modificación indeseada de archivos o del ambiente del sistema, o fallo del sistema. Hay una necesidad de mantener un ambiente conocido y estable para realizar las pruebas significativas en éste y prevenir el acceso inapropiado del desarrollador al ambiente de producción.

Cuando el personal de desarrollo y de pruebas tiene acceso al sistema en producción y a su información, pueden ser capaces de introducir código no autorizado y no probado o alterar datos en producción. En algunos sistemas, esta capacidad podría ser utilizada para realizar fraude, o introducir código no probado o malicioso, que puede causar problemas operacionales serios.

El personal de desarrollo y prueba también representa una amenaza a la confidencialidad de la información operativa. Las actividades de desarrollo y de prueba pueden causar cambios involuntarios al software o a la información si comparten el mismo ambiente. Por lo tanto, es conveniente separar los recursos para desarrollo, prueba y producción para reducir el riesgo de cambio accidental o acceso no autorizado al software en producción o los datos del negocio.

Protección contra código malicioso

Tiene por objetivo el asegurar que las instalaciones de procesamiento de información y la información sean protegidas contra código malicioso.

Controles contra el código malicioso

Se deberían implementar controles de detección, prevención y recuperación, combinados con una adecuada toma de conciencia del usuario, para la protección contra el código malicioso.

La protección contra código malicioso debería basarse en software de detección de código malicioso y software de reparación, en la concientización sobre la seguridad de la información, y en controles apropiados de acceso al sistema y de gestión de cambios. Las siguientes guías deberían considerarse:

a) establecimiento de una política formal que prohíba el uso de software no autorizado;

b) implementación de controles que prevengan o detecten el uso de software no autorizado (por ejemplo, lista blanca de aplicaciones);

c) implementación de controles que prevengan o detecten el uso de sitios web conocidos o sospechosos de ser maliciosos (por ejemplo, listas negras);

d) establecimiento de una política formal de protección contra los riesgos asociados a la obtención de archivos y software tanto por redes externas como por cualquier otro medio, la cual indique las medidas de protección que se deben adoptar;

e) reducción de las vulnerabilidades que podrían ser explotadas por el código malicioso, por ejemplo, a través de la gestión de las vulnerabilidades técnicas;

f) llevar a cabo revisiones regulares del software y contenido de datos de sistemas que soportan los procesos críticos del negocio; la presencia de archivos no aprobados o correcciones no autorizadas debería ser investigada formalmente;

g) la instalación y actualización regular del software para detección de código malicioso y software de reparación, para examinar las computadoras y los medios de forma rutinaria como control preventivo; las verificaciones deberían incluir:
   1) revisión, antes de su uso, de los archivos recibidos a través de redes o por cualquier tipo de medio de almacenamiento en busca de código malicioso;

   2) la revisión, para la detección de código malicioso de todo archivo adjunto a un correo electrónico o de toda descarga antes de su uso; esta revisión se hará en distintos lugares, por ejemplo, en los servidores de correo electrónico, en las computadoras de escritorio y al ingreso a la red de la organización;

   3) la exploración de páginas web para la detección de código malicioso;

h) definición de procedimientos y responsabilidades para manejar la protección contra código malicioso en los sistemas, la formación en su uso, el reporte y la recuperación ante ataques de código malicioso;

i) preparación de planes de continuidad del negocio apropiados para la recuperación ante los ataques de código malicioso, incluyendo todos los respaldos de datos y de software necesarios, así como los planes para la recuperación;

j) implementación de procedimientos para recolectar regularmente información, tales como la suscripción a las listas de correo electrónico o comprobación de los sitios web que brindan información sobre nuevo código malicioso;

k) implementación de procedimientos para verificar la información relativa al código malicioso y asegurarse de que los boletines de alerta sean precisos e informativos; los administradores deberían asegurarse de que se diferencien los avisos reales de código malicioso de los avisos falsos usando fuentes calificadas, como por ejemplo, revistas expertas, sitios de Internet fidedignos o proveedores de software contra código malicioso; todos los usuarios deberían ser conscientes sobre el problema de los falsos avisos de código malicioso y qué hacer en caso de recibirlos.

l) aislar ambientes en los que se pueden producir impactos catastróficos.

El uso de dos o más productos de software de diversos proveedores y tecnología que protegen contra código malicioso en todo el ambiente de procesamiento de la información, puede mejorar la eficacia de la protección contra el código malicioso.

Debería tenerse especial cuidado para protegerse contra la introducción de código malicioso durante los procedimientos de mantenimiento y de emergencia, los cuales pueden evadir controles normales de protección contra código malicioso.

SEGURIDAD DE LAS OPERACIONES

Bajo ciertas condiciones, la protección contra el código malicioso puede causar trastornos en las operaciones.

El uso de software de detección de código malicioso y software de reparación como único control para el código malicioso no es usualmente adecuado y normalmente debería acompañarse por procedimientos operativos que prevengan la introducción del código malicioso.

Respaldo

Tiene por objetivo el proteger contra la pérdida de datos.

Respaldo de la información

Las copias de respaldo de la información, del software y de las imágenes del sistema, deben ser obtenidas y analizadas periódicamente de acuerdo con una política acordada de respaldo.

Debería establecerse una política de respaldos para definir los requisitos de la organización para los respaldos de la información, software y sistemas.

La política de respaldo debería definir los requisitos de retención y protección.

Deberían proporcionarse recursos adecuados de respaldo para garantizar que toda la información y software esenciales se pueden recuperar después de un desastre o falla de medios.

Al diseñar un plan de respaldo, deberían considerarse los siguientes ítems:

a) deberían ser generados registros exactos y completos de las copias de respaldo y de los procedimientos de restauración documentados;

b) la extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos deberían reflejar los requisitos de negocio de la organización, los requisitos de la seguridad de la información implicada y la criticidad de la información para la operación continua de la organización;

c) los respaldos deberían almacenarse en un lugar remoto, a una distancia suficiente para librarse de cualquier daño por un desastre en el sitio principal;

d) la información de respaldo debería tener un nivel apropiado de protección ambiental y física coherente con las normas aplicadas en el sitio principal;

e) los medios de respaldo deberían ser probados regularmente para asegurarse de que pueden ser confiables para su uso en caso de emergencia cuando sea necesario; esto se debería combinar con una prueba de los procedimientos de restauración y comprobados con el tiempo de restauración requerido. La prueba de capacidad para restaurar los datos respaldados debería realizarse en medios de prueba dedicados, y no sobrescribiendo el medio original en caso de que el respaldo o el proceso de restauración falle y cause pérdida o daños irreparables de datos.

f) en situaciones donde la confidencialidad es de importancia, los respaldos deberían protegerse por medios de cifrado.

SEGURIDAD DE LAS OPERACIONES

Los procedimientos operacionales deberían supervisar la ejecución de los respaldos y abordar las fallas de respaldos calendarizados para asegurarse de la integridad de las copias de seguridad de acuerdo con la política de respaldo.

Los planes de respaldo para los sistemas y servicios individuales deberían verificarse regularmente para asegurarse de que cumplen los requisitos de los planes de continuidad del negocio. Para los sistemas y servicios críticos, los planes de respaldo deberían cubrir toda la información, aplicaciones, y datos de los sistemas necesarios para recuperar el sistema completo en caso de un desastre.

Debería determinarse el periodo de retención para la información esencial de la organización, y también cualquier requisito para las copias de archivo a conservarse permanentemente.

Registro y seguimiento

Tiene como objetivo el registrar los eventos y generar evidencia.

Registro de eventos

Se deberían generar, mantener y revisar periódicamente los registros de eventos de las actividades de los usuarios, las excepciones, las fallas y los eventos de seguridad de la información.

Los registros de eventos deberían incluir, cuando corresponda:

a) identificaciones (ID´s) de usuarios;

b) actividades del sistema;

c) fechas, horarios y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión;

d) identidad o ubicación del dispositivo si es posible, y el identificador del sistema

e) registros de intentos de acceso al sistema exitosos y rechazados;

f) registros de intentos de acceso, exitosos y rechazados, a los datos y a otros recursos;

g) cambios en la configuración del sistema;

h) uso de privilegios;

i) uso de utilidades y aplicaciones del sistema;

j) archivos accedidos y tipo de acceso;

k) direcciones y protocolos de red;

l) alarmas emitidas por el sistema de control de acceso;

m) activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y sistemas de detección de intrusos;

n) registros de las transacciones realizadas por los usuarios en las aplicaciones.

El registro de eventos establece las bases para los sistemas de seguimiento automatizados, que son capaces de generar informes consolidados y alertas en la seguridad del sistema. Las bitácoras de eventos pueden contener datos confidenciales e información de identificación personal. Deberían tomarse medidas adecuadas de protección de la privacidad.

Siempre que sea posible, los administradores de los sistemas no deberían tener permiso para borrar o desactivar los registros de sus propias actividades.

Protección de la información de bitácoras
Los recursos para el registro en bitácoras y la información de bitácoras deberían ser protegidos contra la manipulación y el acceso no autorizado.

Se deberían destinar controles para proteger contra cambios no autorizados a la información de bitácoras y problemas con las facilidades de registro en bitácoras, incluyendo:

a) la alteración a los tipos de mensajes que son registrados;

b) los archivos de bitácoras que están siendo editados o eliminados;

c) la capacidad de almacenamiento de los medios de archivo de bitácora que es excedida, resultando tanto en la falla del registro de eventos como en la sobrescritura de eventos anteriormente registrados.

Algunas bitácoras de auditoría pueden ser requeridas para ser archivadas como parte de la política de retención de registros o debido a requisitos para recolectar y retener evidencia.

Las bitácoras del sistema a menudo contienen un vasto volumen de información, mucha de la cual no tiene relación con el seguimiento de la seguridad de la información. Para ayudar a la identificación de eventos significativos para propósitos de seguimiento de la seguridad de la información, debería considerarse la copia automática de los tipos de mensajes apropiados a una bitácora secundaria, el uso de utilitarios del sistema adecuados o herramientas de auditoría para realizar la interrogación y racionalización de los archivos.

Las bitácoras del sistema necesitan ser protegidas, debido a que, si los datos en éstas pueden ser modificados o eliminados, su existencia puede crear una falsa sensación de seguridad. Las copias en tiempo real de las bitácoras a un sistema fuera del control de un administrador u operador del sistema, se pueden utilizar para salvaguardar las bitácoras.

Bitácoras del administrador y operador
Las actividades del administrador y el operador del sistema deberían registrarse en bitácoras, y las bitácoras protegerse y revisarse periódicamente.

Los dueños de cuentas de usuario privilegiadas pueden ser capaces de manipular las bitácoras en los recursos de procesamiento de información bajo su control directo, por lo tanto, es necesario proteger y revisar las bitácoras para mantener la rendición de cuentas de los usuarios privilegiados.

Un sistema de detección de intrusos gestionado fuera del control de los administradores del sistema y de la red, puede ser utilizado para dar seguimiento a las actividades de los administradores del sistema y de la red para efectos de cumplimiento.

Control de software en producción

Tienen como objetivo el asegurar la integridad de los sistemas en producción.

Instalación de software en los sistemas en producción

Deberían implementarse procedimientos para controlar la instalación de software en los sistemas en producción.

Deberían considerarse las siguientes directrices para controlar cambios de software en los sistemas en producción:

a) la actualización de software en producción, aplicaciones, y bibliotecas de programa sólo debería realizarse por administradores capacitados bajo la apropiada autorización de la dirección;

b) los sistemas en producción deberían tener sólo código ejecutable aprobado y no código en desarrollo o compiladores.

c) el software de aplicaciones y el de sistemas operativos debería implementarse sólo después de pruebas extensas y exitosas; las pruebas deberían cubrir la utilidad, la seguridad, los efectos sobre otros sistemas y la cualidad de ser amigable con el usuario, y deberían realizarse sobre sistemas separados; debería asegurarse de que todas las bibliotecas de programas fuentes correspondientes hayan sido actualizadas;

d) debería utilizarse un sistema de control de configuraciones para mantener el control de todo el software implementado, así como de la documentación de sistema;

e) debería establecerse una estrategia de reversión antes de que los cambios sean implementados;

f) debería mantenerse un registro de auditoría de todas las actualizaciones a las bibliotecas de programas en producción;

g) debería conservarse la versión previa de software de aplicación como una medida de contingencia;

h) deberían archivarse las versiones anteriores de software, junto con toda la información requerida y parámetros, procedimientos, detalles de configuración y software de soporte mientras los datos sean conservados en archivo.

El software utilizado en sistemas en producción suministrado por proveedores debería ser mantenido en un nivel soportado por el proveedor. Con el tiempo, los vendedores de software dejarán de dar soporte a las versiones más antiguas. La organización debería considerar los riesgos de confiar en el software sin soporte.

Cualquier decisión de cambio a una nueva versión debería tener en cuenta, los requisitos del negocio para el cambio y la seguridad de la nueva versión, por ejemplo, la presentación de una nueva funcionalidad de seguridad de la información o el número y la severidad de

problemas de seguridad de la información que afectan esta versión. Los parches de software deberían aplicarse cuando pueden ayudar a remover o reducir debilidades de seguridad de la información.

El acceso físico o lógico únicamente se debería dar a los proveedores para propósitos de soporte, cuando sea necesario, y con aprobación de la dirección. Las actividades del proveedor deberían supervisarse.

El software de computador puede depender de software y módulos suministrados externamente, lo cual debería supervisarse y controlarse para evitar cambios no autorizados que puedan presentar debilidades de seguridad.

Gestión de vulnerabilidades técnicas

Tienen como objetivo el prevenir la explotación de vulnerabilidades técnicas.

Gestión de vulnerabilidades técnicas

Se debería obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados, se debería evaluar la exposición de la organización a estas vulnerabilidades y tomar las medidas apropiadas para abordar el riesgo asociado.

Un requisito previo para la gestión efectiva de vulnerabilidades técnicas es un inventario actual y completo de activos. La información específica necesaria para apoyar la gestión de vulnerabilidades técnicas, incluye al proveedor de software, los números de versión, el estado actual de implementación (por ejemplo, qué software está instalado sobre qué sistemas), y las personas responsables del software dentro de la organización.

Una acción apropiada y oportuna debería realizarse en respuesta a la identificación de potenciales vulnerabilidades técnicas. Las siguientes recomendaciones deberían seguirse para establecer un proceso efectivo de gestión de vulnerabilidades técnicas:

a) la organización debería definir y establecer los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo el seguimiento de la vulnerabilidad, la evaluación de riesgo de la vulnerabilidad, la aplicación de parches, el seguimiento de activos, y cualquier responsabilidad de coordinación requerida;

b) los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas relevantes y para mantener la concientización sobre ellas, para el software y otras tecnologías, deberían identificarse (con base en la lista de inventario de activos); estos recursos de información deberían actualizarse basándose en cambios en el inventario, o cuando se encuentren otros recursos nuevos o útiles;

c) debería definirse un plan de acción para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;

d) una vez que ha sido identificada una potencial vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las acciones a ser tomadas; tal acción podría implicar la aplicación de parches a sistemas vulnerables o la aplicación de otros controles;

e) dependiendo de cuán urgentemente necesita ser atendida una vulnerabilidad técnica, la acción a tomar debería realizarse según los controles relacionados con

la gestión de cambio o siguiendo procedimientos de respuesta de incidentes de seguridad de la información;

f) si está disponible un parche de una fuente legítima, los riesgos asociados con su instalación deberían evaluarse (los riesgos derivados de la vulnerabilidad deberían compararse con el riesgo de instalar el parche);

g) los parches deberían probarse y evaluarse antes de ser instalados para asegurarse de que sean efectivos y no causen efectos secundarios que no pueden ser tolerados; si no está disponible ningún parche, deberían considerarse otros controles, como:
    1) desactivar servicios o funcionalidades relacionadas con la vulnerabilidad;

    2) adaptar o agregar controles de acceso, por ejemplo: cortafuegos (firewalls), en el perímetro de la red;

    3) incrementar el seguimiento para descubrir ataques reales;

    4) fomentar conciencia sobre la vulnerabilidad;

h) debería mantenerse un registro de auditoría para todos los procedimientos emprendidos;

i) debería supervisarse y evaluarse con regularidad el proceso de gestión de vulnerabilidades técnicas para asegurar su eficacia y eficiencia;

j) deberían abordarse primero los sistemas de alto riesgo;

k) debería alinearse un proceso efectivo de gestión de vulnerabilidades técnicas con las actividades de gestión de incidentes, para comunicar los datos de las vulnerabilidades a la función de respuesta a incidentes y a establecer los procedimientos técnicos a ser ejecutados si ocurre un incidente;

l) definir un procedimiento para abordar la situación cuando ha sido identificada la vulnerabilidad, pero no existe ninguna contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones detectivas y correctivas adecuadas.

La gestión de vulnerabilidades técnicas puede ser vista como una sub-función de la gestión de cambio y como tal puede aprovechar los procesos y procedimientos de gestión de cambio.

Los proveedores están a menudo bajo la presión significativa de liberar parches cuanto antes. Por lo tanto, existe la posibilidad de que un parche pueda no abordar el problema adecuadamente y tener efectos secundarios negativos. También, en algunos casos, una vez que el parche es aplicado, la desinstalación puede no ser lograda con facilidad.

Si no son posibles las pruebas adecuadas de los parches, por ejemplo, debido a costos o carencia de recursos, puede considerarse una demora en aplicar el parche para evaluar los riesgos asociados, basados en la experiencia reportada por otros usuarios.

SEGURIDAD DE LAS OPERACIONES

Restricciones en la instalación de software
Las reglas que rigen la instalación de software por los usuarios deberían ser establecidas e implementadas.

La organización debería definir y aplicar una política estricta sobre qué tipos de software pueden instalar los usuarios.

Debería aplicarse el principio de menor privilegio. Si se les concede ciertos privilegios, los usuarios pueden tener la capacidad de instalar software. La organización debería identificar qué tipos de instalaciones de software son las permitidas (por ejemplo, actualizaciones y parches de seguridad al software existente) y qué tipos de instalaciones están prohibidas (por ejemplo, software que es sólo para uso personal y software cuyo origen pueda ser potencialmente dañino, desconocido o sospechoso). Estos privilegios se deberían conceder teniendo en cuenta las funciones de los usuarios afectados.

La instalación no controlada de software en los dispositivos informáticos puede conducir a la introducción de vulnerabilidades y luego a la fuga de información, pérdida de integridad u otros incidentes de seguridad de la información, o a la violación de los derechos de propiedad intelectual.

Consideraciones de la auditoría de sistemas de información

Tienen como objetivo el minimizar el impacto de las actividades de auditoría en los sistemas en producción.

Controles de auditoría de sistemas de información
Los requisitos de auditoría y las actividades relacionadas con la verificación de los sistemas en producción deberían ser cuidadosamente planificados y acordados para reducir al mínimo las interrupciones de los procesos de negocio.

Las siguientes recomendaciones deberían tenerse en cuenta:

a) deberían acordarse, con la gerencia apropiada, los requisitos de auditoría de acceso a los sistemas y datos;

b) debería acordarse y controlarse el alcance de las pruebas técnicas de auditorías.;

c) las pruebas de auditoría deberían estar limitadas a accesos de solo lectura al software y a los datos;

d) otro acceso distinto a solo lectura, solamente debería permitirse para copias aisladas de archivos del sistema, que deberían borrarse cuando se complete la auditoría, o bien brindar la adecuada protección si hay obligación de mantener tales archivos como requisito de documentación de la auditoría;

e) los requisitos para procesos especiales o adicionales deberían identificarse y acordarse;

f) las pruebas de auditoría que podrían afectar la disponibilidad del sistema deberían ejecutarse fuera de horas laborales;

g) todo acceso debería ser supervisado y registrarse para producir un rastro para referencia.