UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingenieria Industrial y de Sistemas

AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

INFORME DE INGENIERIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PRESENTADO POR:

MIGUEL EDUARDO ESPINAL LAU

LIMA - PERU

1995

I N D I C E

INTRODUCCIÓN

Este trabajo tiene como objetivo el brindar una visión general de los pasos necesarios para la conducción de una auditoría de seguridad de sistemas de información.

Los problemas de seguridad de información se han venido incrementando en la medida que los sistemas de información están cada día mas integrados con las operaciones en las organizaciones modernas.

Este informe trata en primer lugar de abordar el tema en forma conceptual, para luego especificar algunos procedimientos y puntos claves a considerar en un proceso de auditoría de seguridad de sistemas de información con el objetivo de evitar fraudes o daño de la información en forma casual o intencional.

Por qué es necesario una Auditoría de Seguridad de Información

Es necesario realizar en toda organización moderna una auditoría de seguridad de sistemas de información, debido principalmente a:

- Los sistemas de información están cada vez más presentes en el quehacer diario de la organización moderna.
- Estos sistemas y la información son cada día más accesibles a más personas
- Requerimientos legales obligan a la adopción de medidas de seguridad de la integridad de la información
- La ventaja competitiva de las organizaciones muchas veces radica en la salvaguarda de la confidencialidad de la información
- El continuo cambio en los sistemas requiere que sean continuamente re-evaluados en términos de su habilidad para mantener su integridad

- Es importante determinar el nivel de equilibrio óptimo entre restricción y acceso a fin de que todos puedan trabajar sin amenazar la seguridad del sistema.

Niveles en el Manejo de la Seguridad de la Información

Las necesidades de seguridad de información puede ser dividida en cuatro niveles:

Figura 1

Al primer nivel, las políticas corporativas incluyen controles para la conducción del negocio, como por ejemplo cuales son las herramientas financieras que se deben utilizar para medir la performance del negocio y de cada una de sus áreas.

Al segundo nivel se encuentran los controles de negocio o controles operacionales, los cuales son necesarios para determinar por ejemplo que se adopten los adecuados niveles de inventario, o que se asigne el límite de crédito adecuado para los nuevos clientes.

Estos tipos de controles están basados en el buen funcionamiento de los controles del tercer nivel, llamados controles de sistemas, los cuales incluyen los procesos automáticos y manuales para coleccionar, manipular y almacenar información,

Finalmente, el éxito de toda esta pirámide de controles, dependerá de los controles de infraestructura, los cuales están enfocados en los controles necesarios que se deben contemplar para el acceso físico de las instalaciones y de los equipos de la organización.

¿A quién compete la Seguridad de la Información?

Antiguamente existía una serie de ideas con respecto a la responsabilidad de la seguridad de la información, que se puede resumir en:

- Los “dueños del sistema” era el Departamento de Sistemas, área que centralizaba el funcionamiento y operación de todos los sistemas.
- La tecnología de la información era un Area de Soporte del negocio.
- La función de seguridad de información estaba centralizada en el Departamento de Sistemas.

Actualmente esos puntos de vista han cambiado dramáticamente a tal punto que actualmente es idea generalizada que:

- El “dueño” real del sistema es el propio usuario que utiliza dicho sistema.
- La tecnología de información es pieza fundamental para el funcionamiento del negocio.
- La seguridad de información se debe descentralizar.
- El éxito de un sistema de seguridad de información depende del apoyo para los controles por parte de todos en la organización. Esto es posible lograrlo a través de programas de educación del personal para que entiendan el valor y la importancia del resguardo de la seguridad de la información.

CAPITULO I: COMPLETAR EL ANÁLISIS DE AMENAZAS Y VULNERABILIDAD DEL SISTEMA

Algunas organizaciones inician el proceso de auditoria utilizando las técnicas de análisis de riesgo que requieren un estimado de valores esperados anuales en términos cuantitativos, lo cual implica tener de antemano un costo aproximado de la catástrofe en caso de presentarse un evento inesperado.

Este tipo de técnica es apropiada cuando existren una serie de datos que hacen posible este estimado. Sin embargo, en casos donde la perdida debido a problemas de seguridad es muy complejo determinar, o donde las mayores perdidas aún no han ocurrido, un análisis de amenazas y vulnerabilidades es mucho mas apropiado.

El análisis de amenaza y vulnerabilidad ayuda a los analistas a tener una visión clara de la manera en que la seguridad de la información impacta en términos de negocio.

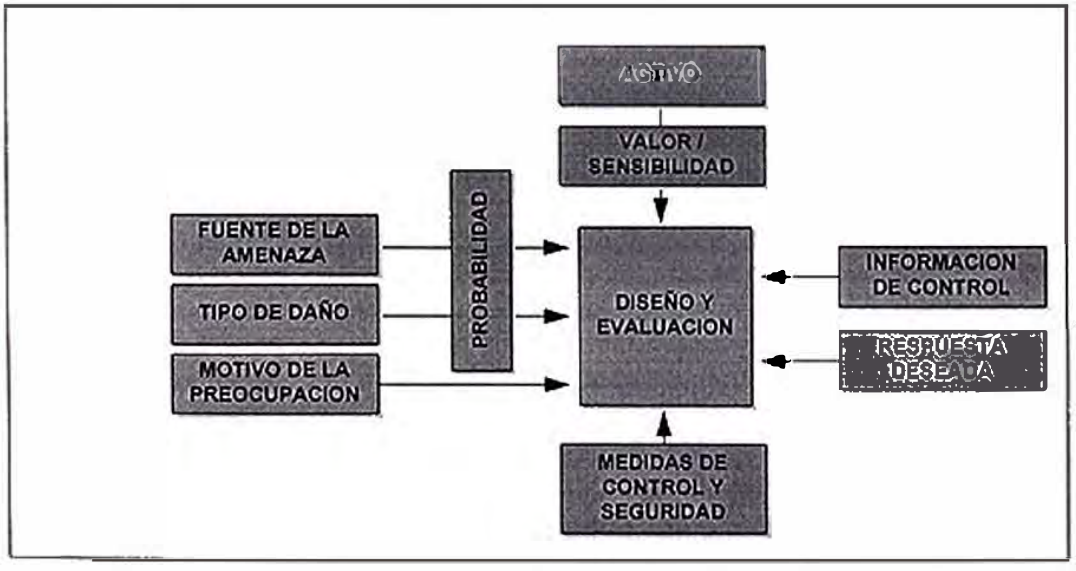

Figura 2

Cuando se evalúa cualquier sistema de seguridad y control, las siguientes preguntas deben ser respondidas:

¿Cuál es el bien que se proteje?

¿Cuál es la fuente de la amenaza?

¿Qué tipo de daño ocurrirá a la empresa si la amenaza se realiza?

¿Por qué existe la preocupación?

¿Qué otros controles existen ante esta amenaza?

¿Cuál es la respuesta deseada?

¿Qué medidas de seguridad y control hay disponible?

La respuesta a cada una de estas preguntas es de igual importancia, y deben ser consideradas cuando las soluciones sean desarrolladas. Por ejemplo, considerar el caso de un sistema de cómputo produciendo cheques para el pago de facturas. El bien que se protege es obviamente el efectivo, un activo bastante atractivo de fácil traslado.

Existe un número de posibles amenazas a la seguridad del sistema de pago de facturas, algunas de las cuales incluyen una cierta confabulación entre el personal interno y externo. El daño a la empresa depende de las sumas implicadas y del giro del negocio. En organizaciones con bajos márgenes de utilidad, pérdidas de cualquier tamaño son consideradas significativas. En este ejemplo, la manera en que los cheques son procesados muestra el porque es importante entender el control de toda la estructura instalada para el pago de las facturas.

Existen varias maneras de cómo un sistema de emisión de cheques puede operar. Por ejemplo, el sistema puede producir un cheque como resultado de que el empleado ingrese una transacción. Los cheques son transferidos al supervisor, quien asegura que cada factura esté autorizada y que los detalles estén correctos antes de firmar los cheques. El

punto de control es la firma de los cheques. Los sistemas mecanizados y controles de infraestructura no deben permitir el pago de facturas fraudulentas o incorrectas.

Otra manera de cómo el sistema puede operar es que el supervisor revise que las facturas sean correctas y autorizadas, ingresando una transacción en el sistema. Entonces el computador automáticamente produce cheques firmados. En este caso, la infraestructura juega una papel importante en el control de los pagos. La seguridad depende de los controles de acceso lógico. Por ejemplo, nadie más que el supervisor debe emitir cheques. Si esta regla es cumplida automáticamente, entonces, la importancia de controles sobre el archivo de datos es considera como adecuada. Pero en este caso, un programador u operador del sistema puede insertar una transacción que aparente ser de las revisadas por el supervisor, el sistema generaría un cheque firmado y el fraude se habría consumado. Este ejemplo proporciona una excelente ayuda para visualizar la importancia que se debe tener al realizar las preguntas anteriormente mencionadas para identificar los riesgos que existen en los procesos del negocio.

Recolección de datos

La mejor fuente de información para conducir la auditoría es entrevistar personas claves de toda la organización.

En muchos casos, el orden de entrevistas debe seguir la estructura de la pirámide descrita en la figura 1. Las personas en posiciones de alto nivel deben ser entrevistadas primero para que el grupo auditor establezca una clara visión del nivel de la política. Una vez que esto haya sido efectuado, otros niveles deben ser entrevistados para enriquecer las conclusiones encontradas en el nivel ejecutivo.

En muchos casos, cada entrevista debe ser conducida por dos miembros del grupo auditor. Una persona puede anotar los comentarios hechos por el entrevistado mientras que otro

dirige la entrevista. Para las entrevistas, el grupo auditor debe revisar completamente los pasos delineados en esta auditoría y formular las preguntas que darán la información necesaria en cada paso.

La siguiente lista proporciona un punto de partida para identificar a los posibles entrevistados.

- El patrocinador de la auditoría (generalmente el director de MSD o IT)
- Ejecutivos de las principales áreas de la organización.
- Funcionario de Seguridad
- Jefe de Desarrollo de Sistemas
- Jefe de Soporte Técnico
- Administrador de Redes
- Jefe de Auditoría Interna
- Jefe de Control de Calidad
- Jefe de Programación

1.1 DETERMINAR EL ACTIVO A PROTEGER

Solo se requiere de control cuando existe un activo que debe ser protegido. Por lo tanto, el objeto que va ser protegido debe ser claramente identificado y entendido, lo que nos llevara a profundizar el mecanismo de control más efectivo.

Existen dos maneras de observar la información como un bien o activo. La información puede tener un valor intrínseco, como en el caso de la base de datos comerciales donde se cobra a los usuarios una cuota por el acceso a la información, o en el caso de sistemas de decisión y soporte gerencial los cuales poseen una gran cantidad de información confidencial que en caso de caer en manos de la competencia, pudiera tener efectos comercialmente desastrosos.

Similarmente, las cifras del balance podrían ser valiosas para los especuladores de la bolsa de valores, si son reveladas antes de que los resultados sean anunciados.

Considerar la correspondencia que probablemente es generada cuando se está efectuando una licitación grande revela otro elemento importante en la evaluación de los sistemas de seguridad. El valor de la información antes de que la licitación haya sido acordada es muy diferente a su valor luego que el trato se haya hecho.

Alternativamente, la información puede ser valiosa porque facilita o previene el acceso a bienes con valor intrínseco. Ejemplos de este tipo de información incluyen inventario o sistemas de control de las provisiones. El acceso al sistema no causará daño directo pero permitirá el robo de los bienes controlados. La importancia de los registros de control de provisiones varía dependiendo en el valor y la liquidez de los bienes.

Realizar las preguntas correctas

cA pesar de que muchos gerentes poseen computadores sobre sus escritorios, pocos de ellos son técnicos expertos. Cuando los gerentes ensayan responder preguntas sobre seguridad de información basados en la tecnología generalmente son incapaces en determinar cuales deben ser las respuestas a esas preguntas.

Por ejemplo, un gerente se ha preocupado acerca de la seguridad de los computadores personales (PC), podría leer un artículo sobre la seguridad de PC's, comprar un paquete y asumir que todos los problemas de seguridad están resueltos. El mismo gerente tal vez no se de cuenta de la necesidad de asegurar el acceso a la red.

Ellos también podrían equivocarse en el control de los procedimientos del usuario, por lo tanto, dejando huecos masivos en la seguridad total. En otros casos podrían instalar un sistema de seguridad que va más allá de las necesidades del sistema actual de seguridad, por lo tanto, invirtiendo mas dinero del necesario.

Sin embargo, la tecnología no es factor importante al establecer o evaluar la seguridad de los sistemas de información. La mejor manera para determinar adecuadamente los controles de una Compañía es considerando el valor de la información que se está procesando. En este tema los gerentes pueden comprender y responder mejor que nadie. El valor de un bien de información en cuestión puede ser determinado por preguntas tales como:

- ¿Que ocurriría si la hoja de costos de una de nuestras últimas propuestas cayera en las manos de la competencia?
- ¿Qué ocurriría si el sistema de pedidos trasmite información incorrecta al almacén?
- ¿Cuál es el impacto en el flujo de caja si no podemos generar débitos directos?

Trabajos para el Equipo de Auditoría

Los miembros de un equipo de auditoría utilizaran la información de las entrevistas y de su propio conocimiento para identificar el impacto sobre el negocio. Estas posibles pérdidas deberían ser clasificadas de acuerdo a su magnitud y también de acuerdo a la posibilidad que estos puedan ocurrir en el sistema de información, esta pregunta debería ser hecha : ¿Cómo podría nuestra efectividad de operaciones ser afectado si este sistema fuera dañado o incapacitado?

Al responder esta pregunta el auditor debería estimular qué daño podría incurrir si esta amenaza es realizada. En general, el tipo del bien y el uso en el cual es puesto determinará la naturaleza de la amenaza al cuál está expuesto. El resultado predecido probable es la más importante variable en la respuesta de esta pregunta. ¿Podría la realización de esta amenaza entorpecer la viabilidad del negocio, o es la urgencia para prevenir una falla de alguna forma?, por lo tanto, una auditoría sobre la seguridad de los sistemas de información debería catalogar cada amenaza de seguridad en términos de daño potencial que podría resultar de su realización.

1.2 DETERMINAR LA FUENTE DE LA AMENAZA

Las computadoras no cometen crímenes o hacen costosos errores; la gente que opera a veces lo hace. La fuente de casi todas las amenazas a la seguridad en los sistemas de información es la gente que interactuan con el sistema en una manera u otra. Cuando se evalúa una posible amenaza a un sistema se deberían hacer las listas completas de los grupos de gentes, quienes podrían modificar, destruir, o permitir el acceso no autorizado a la información. Algunos de estos grupos son describidos en lo que sigue.

Personal de Sistemas o MSD

En su personal incluye operadores de computadoras, analistas de sistemas y programadores, y personal de apoyo. Si su acceso no es controlado, estas personas tienen conocimientos del diseño del sistema, sus debilidades y puntos fuertes. Tal grupo son entrenados y pagados para manipular archivos de información y programas. Si ellos desean abusar de sus posiciones, pueden hacerlo sin ninguna obstrucción.

Un control efectivo contra este problema es el implementar una separación de deberes entre los miembros del grupo. Por ejemplo, los operadores no deberían permitirles modificar programas; al mismo tiempo, a los programadores no se debe dar un acceso sin restricciones a los programas de producción e información. Este control se hace más difícil de reforzar en el ambiente de PC's, donde el usuario puede ser un operador, programador, analista y aún un programador de sistemas.

Los Ingenieros de Redes de Sistemas

Los ingenieros de la red tienen acceso a las facilidades de comunicación de la compañía y pueden mostrar y grabar información de la red usando una datascope. Si los mercenarios son una amenaza a la información de la seguridad, entonces los ingenieros deberían ser considerados como supermercenarios. Los ingenieros de la red pueden empalmar nuevas líneas y terminales en redes y sistemas de distribución, ellos tienen una enorme capacidad de crear problemas en una área de red local (LAN), cualquier usuario con un implemento PC y un paquete de software, le da a él o ella el poder de un ingeniero de red.

Los ingenieros de equipos

Los ingenieros de equipo tiene acceso al hardware y frecuentemente a archivos de disco y grabación. A través de diagnósticos, los ingenieros de equipo podrían dar un vistazo a través de los trabajos internos de las computadoras sin el conocimiento de la Gerencia.

Los Empleados de Servicio del Edificio

Los empleados de servicios no deberían ser olvidados como una amenaza potencial. El personal de servicio usualmente entran al edificio después de horas, cuando hay pocos empleados presentes. Aun sin el acceso al sistema de computación, gente de afuera quien tiene acceso fácil a los edificios podrían obtener información crítica recogiendo copias de impresiones o impresiones descartadas. Una técnica usada por los mercenarios es el "rebuscado en el basurero". Que es rebuscar toda la documentación botada afuera en los tachos de basura, por lo tanto, las medidas de seguridad tomadas en la protección de los sistemas de computación deberían ser aplicadas igualmente a los tachos de basura. Otras personas quienes podrían tener acceso a las oficinas de la Compañía incluye la gente de mantenimiento, gente de reparación, y guardias de seguridad.

Extraños

Casi todos los sistemas recibirán atención de amenazadores extraños, incluyendo mercenarios. El DEC VAX es un frecuente blanco de los mercenarios, y ellos frecuentemente tienen un extensivo conocimiento de hardware y software. Los controles técnicos incluyendo inscripción y controles de acceso lógico, son importantes en la protección de los sistemas de los mercenarios. Sin embargo, estos únicos sistemas no son suficientes. Mercenarios experimentados encuentran relativamente fácil de obtener acceso a la información confidencial. Ellos podrían telefonear a un supervisor de la red o mesa de partes y reclamar que son representantes de alguien de la compañía. A través de este canal, ellos frecuentemente pueden aprender la palabra clave o códigos de acceso. Por lo tanto cuando las personas que tratan con el acceso a este tipo de información confidencial no están entrenados en como regular sus salidas, la integridad del sistema de información es seriamente amenazada.

Otros extraños con fácil acceso incluye consultores, auditores y visitantes casuales tal como gente de reparto y lectores de medidores.

Tareas para el equipo de auditoría

Después de entrevistar a la gente principal de los sistemas de información deberían identificar todas las posibles amenazas de cada información en los bienes listados en el previo paso.

Ellos deberían identificar medidas de seguridad que están en uso corrientemente y estar en guardia contra esas amenazas.

1.3 DETERMINAR EL MOTIVO DE LA PREOCUPACIÓN

La razón del control motivador de cualquier aspecto de un sistema afecta la fuerza del control requerido. Por ejemplo un control designado a efectuar obligaciones legales con multas masivas para los incumplidos, necesitará ser más robusto que un control designado a dar a la Gerencia un sentir de comodidad. Por supuesto, en motivo de proteger el activo debe ser considerada en conjunto con la naturaleza de la amenaza, el valor del bien, etc. Algunas posibles razones para instituir los controles son:

Política de la corporación

Las bases de una buena seguridad es la politica de la seguridad de la compañía. Esta politica es declaración endosada por la Gerencia que da las líneas sobre los requisitos de seguridad en términos generales. Podrían existir otras políticas o reglas internas que tienen requisitos de seguridad.

Legislación

En Europa se han determinado una serie de controles y procedimientos de seguridad como obligatorios para una serie de negocios, para que la información que ellos manejan sea protegida contra accesos no autorizados, alteración y/o destrucción, sea accidental o deliberada. Las medidas que se deben usar no están especificadas, pero los requerimientos son claros.

La política de las sociedades de bancos requiere que los sistemas de computadora se mantengan asegurados. En Europa y Estados Unidos se requiere que todos los operadores de los sistemas de reservación aéreas deban tener una auditoría independiente de seguridad.

Contratos

Hay un crecimiento en el uso del intercambio de data electrónica y banqueo electrónico. Por ejemplo, muchas cadenas de tiendas ahora procesan sus pedidos electrónicamente. Sus abastecedores reciben un pedido en un terminal y someten sus facturas de la misma forma. La gente puede tener acceso a sus cuentas corrientes y pedir transferencias entre ahorros y cuentas corrientes o de cheques.

Estos son solamente dos de los servicios donde cada grupo contratante dependen en la seguridad del otro. Los contratos para tales sistemas frecuentemente hacen de la seguridad y control una obligación. Por lo menos un banco especifica que los clientes usen un sistema electrónico de banqueo, debe observar todas las recomendaciones delineadas en el manual del usuario. Este es un serio compromiso en el ambiente donde pocas personas estudian el manual del usuario.

Estatutos Contables

Auditores externos podrían recomendar acerca de los apropiados niveles de seguridad y control. Al no seguir con estas recomendaciones podría resultar un incremento en pagos de auditoría y por lo tanto podría tener efectos en los costos. Esto es porque los auditores tendrán que probar de acuerdo con sus controles y tendrán que probar muchas transacciones y esto es un proceso mucho más costoso.

Condiciones de seguros

Las compañías de seguros tendrán requisitos específicos para minimizar el fraude y otros riesgos de computadora, como una condición de proveer seguro. De no cumplir con los requisitos de estos podrían significar que no podría darse la protección del seguro.

Comodidad de la Gerencia

Los controles podrían ser introducidos en respuesta a las preguntas hechas por la Acta Gerencial. Mientras el deseo de complacerla a la Gerencia, puede ser una fuerza motivadora, y debería cuidarse de la necesidad para implementar los controles, será primeramente dirigido a los asuntos de negocios que no debe dejar de lado por los deseos de la Gerencia.

Sin un objetivo al desarrollar los controles, las preguntas equivocadas pueden ser preguntadas y respondidas, que finalmente entorpecerá el funcionamiento del sistema. Por ejemplo, un Gerente podría leer un artículo en una revista o ver una serie en la T.V. acerca de espionaje industrial y solicitar que todos los archivos sean codificados para su seguridad.

La amenaza real tal vez no sea de alguien que tenga acceso a la computadora fuera de la Compañía, sino más bien, un usuario no autorizado, abusando los derechos de acceso al sistema. En este caso codificar todos los archivos no es una protección, porque el sistema codifica toda la información antes de presentarlo a los usuarios autorizados.

Tareas para el Equipo de Auditoría

Para cada uno de las amenazas mayores descritos en los pasos previos, el equipo de auditoría debería evaluar la motivación para imponer o mantener los controles. Estas amenazas identificadas deberían ser catalogadas de acuerdo a su importancia, para que ellos sean implementados. Por ejemplo, las medidas de seguridad requeridos por una cadena grande de abastecedores debería tomarse como precedencia sobre las preferencias personales de los señores gerentes.

1.4 IDENTIFICAR LAS INTERRELACIONES DEL SISTEMA

Las medidas de seguridad y control no operan solitariamente. Ellas interactuan con otros elementos del sistema. Consideremos un sistema de cheques para pagar facturas. ¿Necesita el sistema controles rígidos sobre la producción de los cheques? Si los cheques son comparados con autorizaciones y notas de entrega antes de la firma, la respuesta probablemente sea no.

En este caso hay un pequeño riesgo de cheques ficticios, aun sí la computadora los produce. El control es el cheque con la nota de entrega y la autorización de la factura, en este caso, un control efectivo podría ser uno que detecta errores. Si cheques fraudulentos son producidos, ellos no son inmediatamente enviados por correo. Si no están firmados, el banco no los aceptará, si el sistema es cambiado, cosa que la autorización ingresa a un terminal y los cheques son firmados por computador, la situación cambia. En este caso si la computadora produce cheques fraudulentos, ellos saldrán automáticamente y serán aceptados en el banco. Este escenario requiere de un control que prevenga la producción de cheques fraudulentos.

Tareas para el Equipo de Auditoría

Los miembros del equipo de auditoría deberían trazar la interdependencias de las amenazas primarias que han sido identificados en los previos pasos de la auditoría. Este trazo debería incluir el sistema amenazado, y todos los sistemas que interactúan con él directamente.

Las siguientes preguntas deberían ser respondidas por cada una de los sistemas amenazados:

¿Qué controles se tienen para este sistema?

¿Ellos cuidan las amenazas que han sido identificadas?

¿Qué otros sistemas son afectados por el sistema amenazado?

¿Que efecto tendría un cambio de control para este sistema o los sistemas relacionados?

1.5 DETERMINAR LA RESPUESTA ADECUADA

Cualquier medida de control puede ser generalmente clasificada dentro de 5 amplias categorías, siendo estos:

- Preventiva
- Detectiva
- Reductora de daños.
- Investigación.
- Confirmatoria

El valor del bien en riesgo influirá en el tipo de control a imponer en un sistema. Por ejemplo, bienes de autovalor que deberían ser protegidos por controles que previenen que la amenaza ocurra. Considerar el ejemplo de un transportador de carros. Muchos años atrás la tragedia golpeó cuando un transportador salió de Zeebrugge en Bélgica antes que sus puertas de la proa fueron cerradas. El riesgo de navegación es claramente alto cuando el buque no está listo para el mar. La consecuencia de una falla hace esencial prevenir tales fallas del sistema. En otro sistema el detectar la falla a tiempo para tomar una acción correctiva, podría ser adecuado. Cada uno de los cinco tipos de controles es descrito más adelante.

Preventivo

Los controles preventivos son diseñados para asegurar que tales eventos no deseados no ocurran. Casi todas las medidas de control y seguridad son diseñadas con el objetivo de prevención. Las medidas preventivas frecuentemente imponen restricciones sobre el acceso y uso. Si los controles no están bien designados, ello incrementan los costos, produciendo ineficiencia. Incluido en este tipo de control son ambos, accesos de inscripción: lógico y físico.

Detectivo

Los controles detectivos son invocados después que un evento no deseado ha ocurrido. Estos controles son diseñados para activar una alarma, cosa que la acción correctiva sea tomada. Dependiendo de la sensibilidad del sistema y la naturaleza de la amenaza, controles detectivos son frecuentemente una alternativa satisfactoria para los controles preventivos, usualmente menos obstructivos. Los detectores de humo proveen de un clásico ejemplo de un efectivo sistema de detección.

Reducción de daños

Los controles que limitan el daño cuidan contra las fallas de los controles preventivos. Al tiempo que el problema es descubierto, podría ser demasiado para limitar su impacto, aunque las limitaciones del daño podrían tener efectos negativos al problema, sean minimizados. Tal vez el mejor ejemplos de controles de reducción de daños es un plan de recuperación y contingencia.

Requisitos para mantener un cuarto de computadoras ordenadas, y colocar un aviso de no fumar son medidas preventivas; una alarma de humo sería un control detectivo. Si ambas de estas medidas fallan, de todas manera el fuego empezará, entonces un efectivo plan de recuperación puede limitar el daño al negocio.

Investigación

Un control de investigación no puede prevenir o detectar el problema. Su rol es ayudar a responder preguntas después que el problema ha ocurrido. Un buen ejemplo de un control de investigación es la caja negra que lleva todo avión comercial. Eso es usado por los investigadores del accidente después del mismo para reconstruir los últimos minutos de vuelo. Este mecanismo graba información clave, tal como la altitud, velocidad, y los controles de mando. En sistemas de información, los controles de este tipo incluyen los job log y journal system.

Confirmatoria

Los controles de confirmación son los últimos grupos que son diseñados para confirmar una acción que ha tomado lugar. La falta de controles confirmatorios no llegan directamente a incurrir en fraude o pérdida, pero controles inadecuados de este tipo podría permitir que el sistema sea vulnerable. Ejemplos de controles de confirmación incluyen registros de aceptación de una transacción de un terminal, y registros de control de stock.

Tareas para el Equipo de Auditoría

El equipo de auditoría debería analizar cada uno de las amenazas de seguridad primarias en términos de tipo de respuesta deseada. El tipo de respuesta necesitada depende en el posible daño si la amenaza es realizada. Por ejemplo, un potencial de daño más alto deberían ser cuidadas con medidas preventivas, mientras los daños menores podrían ser minimizados con medidas confirmatorias o de investigación. Los bienes deberían ser catalogados de acuerdo al tipo de control que se necesita.

1.6 DETERMINAR LAS MEDIDAS DE SEGURIDAD Y CONTROL DISPONIBLES

El sexto factor a ser considerado son el tipo de medidas de control que deberían o podrían ser implementados. Los controles son necesarios en cinco áreas:

Personal

Cualquier control puede ser evitado, si las personas responsables por su efectividad son negligentes o maliciosas. Esto es una razón crítica que la Gerencia debe ser sometida a ciertos controles. Los controles de personal incluyen procedimientos de ingreso y despidos, políticas de la organización, estructura del negocio, y sistemas de entrenamiento y evaluación.

El personal podría cometer fraude por razones financieras, o dañar la información del sistema como resultado de un resentimiento contra la compañía.

Uno de los más efectivos controles de este tipo es que las funciones sensitivas del negocio sean manejadas por dos personas, en donde cada persona controlará la integridad del otro.

Procedimiento

Una efectiva manera de cuidado contra el error humano o intensiones dañinas es documental un procedimiento formal para trabajos donde los bienes están en riesgo. Los procedimientos formales permiten que los controles se consideren el punto adecuado.

Cuando un problema serio ocurre, la existencia de un procedimiento equipa a la gente con conocimientos acerca de cómo actuar ante una posible amenaza.

Físico

Anteriormente el cuarto de computación se estaba frecuentemente en el piso de abajo con ventanas muy grandes. Casi todas las compañías ahora reconocen la necesidad de proteger el centro de datos como si fuesen un fortín. Manteniendo la gente no autorizada lejos del activo, es una manera efectiva de asegurarlo.

Técnico

Controles técnicos incluyen accesos lógicos y controles programados, tales como rutinas de validación de data, controles de comunicación como dial-back automático. Estos controles cuando están correctamente instalados son confiables y consistentes. Sin embargo, su efectividad frecuentemente depende de otros controles los cuales podrían apoyar o comprometer los controles técnicos. Por ejemplo, la encriptar los archivos no tiene sentido si los reportes emitidos por el computador salen fácilmente del edificio.

Documentación

El sistema de documentación de procedimientos es la mejor manera de asegurar que ésta se mantenga consistente. El personal nuevo aprenderá como el trabajo es hecho a partir del manual de procedimientos y no tanto de entrenamiento oral, haciendo la instrucción más consistente.

Los sistemas de programas son más fáciles de mantener si la documentación es adecuada en caso contrario será más costoso su mantenimiento.

Tareas para el Equipo de Auditoría

El equipo de auditoría debería evaluar cada amenaza para determinar qué tipo de controles es necesario para cuidar el sistema contra daño o fraude. Determinar las necesidades de seguridad debe involucrar realizar una revisión del tipo de control para cada bien.

1.7 INTEGRACIÓN DE LA DATA OBTENIDA DEL ANÁLISIS DE AMENAZAS Y VULNERABILIDAD

Completando la tabla en la figura Nº3, permitirá que el equipo de auditoría integre la información recolectada. La primera fila de cada columna resume los pasos de esta parte de la auditoría. La segunda fila provee puntos claves que pueden haberse concluido por el análisis desarrollado.

Figura 3

TABLA DE INTEGRACION DE INFORMACIÓN

BIEN / ACTIVO	AMENAZA	MOTIVO DE PREOCUPACIÓN	CONTROLES EXISTENTES / SISTEMAS INTER RELACIONADOS	RESPUESTA APROPIADA	MEDIDAS DE CONTROL DISPONIBLE
¿Qué impacto tendría en el negocio si la amenaza se realizara?	El personal de sistemas La red de ingenieros. Ingenieros de equipo. Personal de servicios de edificios. Otros	Política Corporativa. Legislación Contratos Estatutos contables. Condiciones de seguros. Conformidad de la Gerencia	¿Los controles que están en el lugar son dirigidos a la amenaza? ¿Cómo se afectarían otros sistemas cambiando estos controles?	Preventiva Detectiva Reducción de daños. Investigativa Confirmatoria	Personal Procedural. Físico Técnico Documentación

Completar este ejercicio servirá a los siguientes propósitos:

- Asistir al equipo identificando las prioridades de seguridad de información. Las áreas prioritarias deberían ser aquellos que tendrían un mayor impacto si la amenaza es realizada
- Organizar la información de auditoría en la manera que la acción del planeamiento sea fácil.
- Comprender que tipo de controles son necesitados y en cuáles áreas.

Conduciendo la primera parte de la auditoría ayudará a los responsables del sistema de seguridad a comprender las debilidades y fortalezas en sus sistemas y de priorizar los controles de información. En esencia, una exploración total de estas preguntas ayudará a los gerentes y especialistas de información a comprender las necesidades de seguridad en la parte superior de la pirámide en Figura Nº1, sin embargo como se mencionó anteriormente, el éxito de los controles en todos los niveles dependerá en los controles efectivos al final de la infraestructura.

CAPITULO II: EVALUACIÓN DE LA SEGURIDAD DE LA INFRAESTRUCTURA DE LAS TECNOLOGÍAS DE INFORMACIÓN

Estos cuestionarios están dirigidos a los componentes de un sistema de información. La respuesta a estas preguntas requerirá una investigación detallada de parte de la Gerencia de Sistemas. Es recomendable que esta inspección sea hecha por lo menos anualmente.

2.1 HARDWARE

Satisfacer las demandas de procesamiento es crucial para la seguridad. Las fallas de hardware son una causa común de pérdida o daño de un sistema computacional. El monitoreo de performance, el mantenimiento preventivo, y el rastreo y análisis de fallas de hardware son medidas que pueden asegurar la confiabilidad del hardware. Las siguientes preguntas ayudan a evaluar la suficiencia del hardware de una organización:

¿El plan de adquisición de hardware de la compañía es consistente con el plan del negocio? El plan de adquisición de hardware de la compañía debe soportar la dirección del negocio. Por ejemplo, si el plan de negocio de la compañía contempla una estrategia de tecnología cliente-servidor, entonces el plan de adquisición de hardware debe ser consecuente con dicha estrategia. En otras palabras, la estrategia de adquisición de hardware debería consistir en la compra de PC's cliente-servidor y no de un mainframe.

SI ❑ NO ❑

¿La performance y capacidades del hardware son monitoreadas y reportadas en términos oportunos?

SI ❑ NO ❑

¿Se han programado mantenimientos de rutina periódicos al hardware para reducir la posibilidad y el impacto de fallas?

SI ❑ NO ❑

¿Cómo se registran, analizan y resuelven los problemas de hardware?

SI ❑ NO ❑

Los problemas de hardware deberían ser reportados en un sistema de reportes de mantenimiento, que asigne un número de ticket de problema a cada problema. El análisis del problema puede tener lugar off-line con ingenieros de sistemas. La solución del problema debería ser ingresada en el sistema de reportes de mantenimiento y el ticket de problema debería ser removido del status "pendiente".

¿Cuenta la compañía con un sistema de reportes de mantenimiento?

SI ❑ NO ❑

¿Cuán rápido se resuelven los problemas de hardware?

La rapidez con la que se resuelven los problemas de hardware está en función de la confiabilidad del sistema y la especificación del Tiempo Promedio de Reparación (Mean Time To Repair - MTTR). Por ejemplo, un sistema con un requisito de 99.999 por ciento de disponibilidad debe estar disponible durante todas, salvo 8.76 horas del año. Si el MTTR promedio para este sistema es de 10 horas, entonces el MTTR está fuera de especificación.

¿Los problemas de hardware se resuelven dentro de un plazo aceptable?

SI ❑ NO ❑

¿Cómo se prueban, programan, documentan y aprueban los cambios en la configuración del hardware?

Los cambios en la configuración del hardware deberían ser documentados en un plan de implantación y en un software de control de configuración. El plan de implantación contemplará las pruebas y proveerá de documentación para soportar los cambios en el hardware y la aprobación de los cambios.

¿Cuenta la compañía con un procedimiento documentado para probar cambios en el hardware?

SI ❑ NO ❑

Puntaje: Anótese un punto por cada pregunta respondida con un "SI".

Puntaje total para los controles de seguridad de hardware: 6

Puntaje de la evaluación:

2.2 CONTROLES DE MEDIOS MAGNÉTICOS

¿Quién es responsable por la administración de medios magnéticos y cómo se lleva ésta a cabo?

La responsabilidad por la administración de medios magnéticos recae dentro del área de Sistemas de Información. La manera como se administran los medios magnéticos depende de los procedimientos preferidos por el área de Sistemas de Información. Un estatuto de procedimientos debería cubrir como mínimo las siguientes áreas:

- Cómo deben establecerse y mantenerse las discotecas.
- Cómo deben establecerse y mantenerse las cintotecas.
- Cómo deben realizarse los backups a discos y cintas.
- Dónde deben guardarse los backups.
- Con qué frecuencia deben probarse los backups.

¿La compañía posee una política que cubra la administración de medios magnéticos?

SI ❑ NO ❑

¿Cuándo y cómo se realiza el inventario de la biblioteca de medios magnéticos?

En muchos casos, el inventario de la biblioteca de medios magnéticos se realizará manualmente. Sin embargo, con el surgimiento de nuevas tecnologías, ahora es posible tenerlo completamente automatizado, especialmente con cassettes de cinta. Si el inventario es automatizado, puede ser continuamente actualizado. Si no es automatizado, debería actualizarse cada dos semanas.

¿Se realiza un inventario a la biblioteca de medios magnéticos cada dos semanas?

SI ❑ NO ❑

Puntaje: Anótese un punto por cada pregunta respondida con un "SI".

Puntaje total para los controles de seguridad de medios magnéticos: 2

Puntaje de la evaluación: _____

2.3 SEGURIDAD DE ACTIVOS FÍSICOS

La seguridad de activos físicos es probablemente uno de los aspectos de la seguridad de sistemas de información más ampliamente comprendidos. Sin embargo, existen algunos temas relativos a la seguridad de información que pueden no resultar tan obvios.

¿Los controles son los adecuados para asegurar que la propiedad física de la organización no sea objeto de robo o vandalismo?

Tales controles incluyen el inventario y etiquetado de equipos, ambientes con cerraduras, acceso restringido a áreas con equipo sensible, y ambientes custodiados.

SI ❑ NO ❑

¿Los códigos de identificación están grabados y guardados en un área segura?

SI ❑ NO ❑

¿Los medios de transmisión están adecuadamente protegidos?

SI ❑ NO ❑

¿Están los servidores de la LAN o la red localizados en ambientes con cerraduras y protegidos de oscilaciones de voltaje?

SI ❑ NO ❑

¿Existe un control de acceso físico a sistemas sensibles?

SI ❑ NO ❑

¿Las terminales proveen de números de ID de terminales o números de secuencia de entrada a una aplicación?

SI ❑ NO ❑

Los métodos existentes para este tipo de seguridad incluyen: encriptado, dial-back, y hardware tokens

¿La seguridad del dial-up o de terminales remotos está protegida por alguno de estos métodos?

SI ❑ NO ❑

¿Cómo ha sido implantada y probada la recuperación de desastres?

En sistemas complejos, el desarrollo de un plan de recuperación de desastres es crítico para el éxito a largo plazo. Un plan de recuperación de desastres contempla cada una de las contingencias que pueden enfrentarse en una crisis, tales como:

- Dónde está localizado el backup site
- Cómo se han redirigido las telecomunicaciones para utilizar backup site
- Si el backup site está "caliente" (listo para operar inmediatamente); "tibio" (listo para operar dentro de 24 horas); o "frío" (listo para operar dentro de una semana)

Probar el plan de recuperación de desastres es también crítico para su éxito. Las pruebas pueden ser divididas en al menos cuatro diferentes categorías:

- Pruebas de locación e infraestructura
- Pruebas de telecomunicaciones
- Pruebas de aplicaciones y sistemas
- Pruebas de poder

Debe escribirse un guión para describir las expectativas ante cada uno de estos tipos de pruebas, y para evaluar los resultados de dichos tests. Todas las cuatro categorías deben ser probadas simultáneamente al menos una vez cada seis meses.

¿Se han implantado procedimientos de recuperación de desastres?

SI ❑ NO ❑

¿Los procedimientos de recuperación de desastres se prueban con regularidad?

SI ❑ NO ❑

Puntaje: Anótese un punto por cada pregunta respondida con un "SI".

Puntaje total para los controles de seguridad de medios magnéticos: 10

Puntaje de la evaluación: _____

2.4 SOFTWARE

La evaluación de la seguridad de software involucra varias grandes categorías de software.

La evaluación ha sido dividida en las siguientes secciones:

- Sistemas operativos
- Sistemas aplicativos
- Redes
- Controles lógicos de acceso

Cada categoría será evaluada separadamente.

2.4.1 Sistemas Operativos

Los sistemas operativos proveen la interfase entre los sistemas aplicativos y el hardware. Los sistemas operativos frecuentemente proveen herramientas que permiten a los programadores saltarse los controles de la aplicación y controles del negocio. Esto es porque los sistemas operativos funcionan a los niveles más bajos de un computador. Las preguntas de esta sección revelarán cuán conscientes están los miembros del staff de soporte técnico acerca de la seguridad y el control, y qué pasos han tomado para proveer una adecuada seguridad.

¿Mediante qué procedimiento se identifica, selecciona, programa, prueba, implementa, mantiene y controla la configuración del software de los sistemas operativos?

Esto está representado por el control de configuración y la metodología de desarrollo de sistemas. El control de configuración identifica el software de los sistemas operativos seleccionado, implantado y mantenido. La metodología de desarrollo de sistemas identifica la técnica usada para desarrollar. o programar, las aplicaciones del sistema. El control de configuración debe también ser aplicado a la fase de desarrollo para asegurar una apropiada prueba de configuración.

¿Cuenta la compañía con un control de la configuración de sistemas operativos?

SI ❑ NO ❑

¿La compañía sigue una metodología de desarrollo de sistemas?

SI ❑ NO ❑

¿Qué impacto tiene el sistema operativo sobre la confidencialidad, integridad y disponibilidad de la data y las aplicaciones?

El sistema operativo puede afectar la confidencialidad, integridad y disponibilidad de la data y las aplicaciones. Si no provee confidencialidad, cualquiera puede acceder a la data y el sistema se torna bastante inseguro. Si no provee integridad, no se puede confiar en el sistema para proveer la data adecuada. Si la disponibilidad de la data y las aplicaciones está obstruida, entonces el sistema es de ninguna utilidad.

¿El sistema operativo provee confidencialidad, integridad, y disponibilidad de la data y las aplicaciones?

SI ❑ NO ❑

¿Se ha provisto a los terminales de la consola maestra con un control de acceso físico y lógico adecuado para prevenir el acceso no deseado al sistema operativo?

SI ❑ NO ❑

¿Se han cambiado las contraseñas de instalación del sistema operativo?

SI ❑ NO ❑

Un error común en la instalación de nuevos sistemas es mantener inalterada la contraseña del administrador del sistema de la establecida por defecto por el fabricante. Para aliviar esta preocupación, todas la contraseñas deben ser cambiadas inmediatamente después de la instalación del sistema

SI ❑ NO ❑

¿Qué documentación define quién tiene acceso al núcleo del sistema operativo?

Los procedimientos estándar de operación deben definir a todos los usuarios con acceso privilegiado al núcleo.

¿La compañía cuenta con procedimientos estándar que definan a todos los usuarios con privilegios de acceso al núcleo?

SI ❑ NO ❑

Puntaje: Anótese un punto por cada pregunta respondida con un "SI".

Puntaje total para los sistemas operativos: 6

Puntaje de la evaluación: _____

2.4.2 Sistemas Aplicativos

¿Los programas de las aplicaciones contienen provisiones que rutinariamente verifican el trabajo desempeñado por el software?

SI ❑ NO ❑

¿Las aplicaciones incluyen razonables opciones por defecto?

SI ❑ NO ❑

¿Los programas de las aplicaciones generan totales de control y realizan reconciliaciones para verificar la culminación del proceso?

SI ❑ NO ❑

¿Se han establecido políticas y procedimientos para la asignación de roles y responsabilidades en la administración del ambiente de la base de datos?

SI ❑ NO ❑

¿Se han implantado otros programas de software de control de acceso con el sistema aplicativo?

SI ❑ NO ❑

¿Cómo se administran estos otros paquetes de software de control de acceso? Generalmente, una persona específica es asignada como el administrador de seguridad del paquete de software de control de acceso. Esta persona es responsable por la administración, operación y mantenimiento del programa de seguridad en el día-a-día.

¿Cuenta la compañía con un administrador de seguridad dedicado

SI ❑ NO ❑

¿Qué aplicaciones son compartidas con terceros (otras áreas con acceso a los sistemas)? Compartir aplicaciones con terceros puede ser muy riesgoso. En tales situaciones, la data puede ser completamente expuesta al tercero mientras está en el sistema. Los controles pueden estar usualmente establecidos para prevenir que incluso terceros confiables ganen acceso a data valiosa.

¿Están las aplicaciones adecuadamente protegidas de terceros?

SI ❑ NO ❑

¿El sistema incorpora un Sistema de Detección de Intrusiones para automáticamente reportar comportamientos inusuales del sistema o de los usuarios en el computador?

SI ❑ NO ❑

Entre las herramientas de diagnóstico de problemas en la red, ¿existe una caja de herramientas (toolbox) de seguridad de red? La caja de herramientas debe incluir las siguientes funciones:

- Comparación automática de configuración
- Validación automática de los mecanismos de control de acceso
- Revisión automática del archivo de rastreo (log file) del sistema para la detección de anormalidades
- Detección automática de virus
- Verificación automática de contraseñas

- Verificación automática de identificaciones de usuario para la detección de patrones de acceso reciente

¿El sistema provee todas estas herramientas de diagnóstico?

SI ❑ NO ❑

Puntaje: Anótese un punto por cada pregunta respondida con un "SI".

Puntaje total para los sistemas aplicativos: 9

Puntaje de la evaluación: _____

2.4.3 Redes

La tendencia en sistemas se orienta hacia la computación distribuida, o el enlace de un número de computadores individuales en una red. Las redes inseguras o no controladas pueden permitir el acceso desautorizado a programas e información. Las debilidades de la red son un blanco favorito de los hackers. Las auditorías de seguridad deben prestar particular atención a cuestiones relativas a redes.

¿Se emplean estándares en la definición de las funciones de control de hardware y software requeridas por las redes?

El uso de estándares en definir las funciones de control de software y hardware puede ser desorientador. Ciertamente los estándares de un organismo internacional tal como la IEEE, ANSI, o CCITT pueden ser confiables. Sin embargo, estándares de organismos menos conocidos pueden llevarlo a uno a tener un falso sentido de seguridad

SI ❑ NO ❑

¿Existen procedimientos disponibles que definan las medidas de control y seguridad a ser usadas con las redes de la organización?

SI ❑ NO ❑

¿Se ha establecido una función centralizada para controlar el uso de facilidades de red y la data en la red?

SI ❑ NO ❑

¿Se realizan inventarios de activos de red en todas las localidades y se los actualiza periódicamente?

SI ❑ NO ❑

¿Se han establecido requerimientos de disponibilidad de red, reportes, tiempo y respuesta, backup y control operacional para todas las aplicaciones?

SI ❑ NO ❑

¿Se realizan backups a todo el hardware, software y data de otras localidades?

SI ❑ NO ❑

¿El backup de la data puede ser transmitido a donde y cuando se lo necesite en el tiempo?

SI ❑ NO ❑

¿Están los procedimientos operacionales a punto en caso de una reparación, o el hardware de switcheo de telecomunicaciones en caso de un backup de la red?

SI ❑ NO ❑

¿El acceso a las facilidades de procesamiento de la red está apropiadamente definido y controlado?

SI ❑ NO ❑

¿Se han establecido mecanismos para monitorear y medir el desempeño de la red?

SI ❑ NO ❑

¿Cuáles son las directrices para encriptar data, y cuán efectivas son éstas?

Las directrices para encriptar data deben incluir:

- Qué data debe ser encriptada

- Cuándo debe ser encriptada
- El algoritmo a usar al encriptar
- Sensibilidad de la data
- Cómo se mantienen y distribuyen las claves de encriptamiento

El cuándo encriptar debe ser descrito ya sea en términos de tiempo en un día o siempre. La sensibilidad de la data puede variar desde ser muy sensible, como en el caso de los números de PIN de las transacciones ATM, hasta ser nada sensible en absoluto, como sucede con las cifras de ventas de diez años atrás. La sensibilidad de la data debe ser medida en la lista de ítems a ser encriptados.

¿Se han establecido directrices para encriptar data?

SI ❑ NO ❑

¿Es efectivo el algoritmo de encriptamiento de data?

El algoritmo escogido debe tener una robustez probada. Como ejemplos tenemos la Llave Pública de encriptamiento DES o la RSA. Están disponibles otros algoritmos y debieran bastar por un corto período, pero DES o RSA son los más efectivos algoritmos a largo plazo.

SI ❑ NO ❑

¿La seguridad de la red es la adecuada para proteger las facilidades físicas de la red?

Esta pregunta se refiere principalmente a la seguridad física del equipo de la red.

¿Se ha tenido cuidado de asegurar los ambientes de telecomunicaciones, del servidor, comunicaciones y de facilidades?

SI ❑ NO ❑

¿La seguridad de la red es la adecuada para proteger la integridad del software de aplicación?

La seguridad de la red puede ser implementada de forma tal que sólo aquellos con controles de acceso específicos puedan acceder a las aplicaciones. La seguridad de la red puede requerir un "Logon" de Red - una contraseña requerida antes que se le otorgue a uno el acceso a la red. En este caso, el usuario que desea ingresar a la red tendrá despejado el acceso una vez que ingrese la contraseña correcta. Las Listas de Control de Acceso a la Red controlarán la accesibilidad e integridad de las aplicaciones.

SI ❑ NO ❑

¿La seguridad de la red es la adecuada para proteger la integridad del sistema operativo?

No todos los usuarios de la red deben tener autorizado el acceso al sistema operativo. Las Listas de

Control de Acceso a la Red deben ser establecidas para describir exactamente quién tiene acceso a qué, incluyendo el sistema operativo.

SI ❑ NO ❑

¿Es la seguridad de la red adecuada para proteger el ingreso y salida de datos?

Un técnico sofisticado podría redirigir el ingreso de datos a su pantalla o a la impresora sin que la persona que ingresa los datos lo note. Estrategias similares podrían ser usadas con la salida de datos. Adicionalmente, la seguridad de las impresoras conectadas a la red y la data que arrojan debería ser protegida.

SI ❑ NO ❑

¿Se revisa periódicamente la seguridad de la red en todas las localidades?

SI ❑ NO ❑

¿Existen estándares de LAN dentro de la organización?

SI ❑ NO ❑

¿Los procedimientos a seguir al diseñar y seleccionar una LAN están definidos y documentados?

SI ❑ NO ❑

¿Existe el suficiente manejo y soporte para asegurar la ininterrumpida y confiable operación de la LAN?

SI ❑ NO ❑

Esto se refiere a la política de operaciones de la LAN. ¿Cuán grave debe ser una situación antes de que se permita a la LAN dejar de estar en operación? La política debe incluir cuando usar fuentes de energía ininterrumpidas, mirroring de discos, backups de archivos y servidores de red, backup de telecomunicaciones, y terminales de backup o PC´s.

SI ❑ NO ❑

¿Se ha implantado un control de la configuración de la LAN? Si es así, ¿Cómo ha sido esto logrado

SI ❑ NO ❑

¿Se puede revisar una matriz de perfil de acceso para asegurarse de que los privilegios de acceso otorgados se hayan basado en la necesidad de saber del usuario de la LAN?

SI ❑ NO ❑

¿Existe un "logon" de red único para prevenir el ingreso o acceso desautorizado a la red?

SI ❑ NO ❑

¿Existe alguna facilidad de autenticidad para verificar la referida identidad de un cliente o servicio?

SI ❑ NO ❑

¿Existe segmentación en la red para prevenir el acceso desautorizado a través de las redes y las sub-redes?

SI ❑ NO ❑

¿Alguno de los sistemas de la compañía tiene acceso a y desde Internet?

SI ❑ NO ❑

¿Cómo se controla el acceso a y desde Internet?

El acceso a y desde Internet puede ser controlado por un ruteador aislante junto con un mail forwarding host. Esto debe proteger a la organización usuaria de intrusos procedentes de Internet. De manera similar, los usuarios de la organización que intenten usar el Internet deben ser pre-aprobados y deben registrarse sus direcciones en el ruteador aislante y el mail forwarding host antes de que reciban acceso al Internet.

¿Existen controles de acceso bi-direccional para el acceso a Internet?

SI ❑ NO ❑

Puntaje: Anótese un punto por cada pregunta respondida con un "SI".

Puntaje total para redes: 29

Puntaje de la evaluación: _____

2.4.4 Control Lógico de Acceso

Los controles lógicos de acceso son controles automatizados que limitan el acceso a los recursos de información a personas autorizadas por propósitos autorizados. En algunos casos, existe además un requerimiento de restringir el acceso por hora del día y por localidad. Los controles lógicos de acceso son clave para los sistemas accesados por terminales de computadora. En una instalación bien hecha, uno puede esperar encontrar políticas de seguridad que gobierne las reglas de acceso, procedimientos y herramientas. Ellas deberían cubrir el otorgamiento de acceso, el monitoreo de intentos de acceso desautorizados, y el mantenimiento y uso de contraseñas.

¿Existen controles lógicos de acceso para todos los puntos de acceso al sistema?

SI ❑ NO ❑

¿Quién es responsable por los controles lógicos de acceso?

Generalmente, la responsabilidad por los controles lógicos de acceso pertenece al Administrador de Seguridad. Si no existe un administrador de seguridad, entonces la responsabilidad recaerá en el Administrador del Sistema.

¿Cuenta la compañía con una persona responsable por los controles lógicos de acceso?

SI ❑ NO ❑

¿La política de seguridad de información define las responsabilidades de los usuarios, la dirección y los administradores de la seguridad con respecto a los controles lógicos de acceso?

SI ❑ NO ❑

¿Los usuarios, la dirección y los administradores de la seguridad comprenden sus tareas?

SI ❑ NO ❑

Las tareas relativas a la seguridad deben ser definidas por un funcionario de seguridad de información - una persona a la que se le asigne la responsabilidad de supervisar la implantación de la seguridad en la organización.

SI ❑ NO ❑

¿Están los usuarios, la dirección, y los administradores de la seguridad conscientes de la importancia de los controles lógicos de seguridad de la información y en conformidad con la política de seguridad de información de la organización?

SI ❑ NO ❑

¿Se ha identificado la necesidad de controles lógicos de acceso?

SI ❑ NO ❑

¿Todos los procedimientos de seguridad cumplen con los estatutos o reglamentos aplicables de protección de la privacidad?

SI ❑ NO ❑

¿Cuáles son las reglas de la organización referentes al uso de contraseñas, acceso y otras restricciones lógicas a archivos de datos, sistemas operativos, programas de procesamiento de aplicaciones, y comandos específicos?

Las reglas referentes al uso de contraseñas y otras restricciones lógicas deben estar definidas en una política corporativa de seguridad de información.

¿La compañía define las reglas referentes al uso de contraseñas y otras restricciones lógicas a archivos de datos, sistemas operativos, programas de procesamiento de aplicaciones, y comandos específicos?

SI ❑ NO ❑

¿Cuál es el procedimiento para añadir, cambiar, y eliminar límites de control de acceso? Este debe generalmente ser un procedimiento escrito solicitando a los individuos someter sus reclamos de cambio en el control de acceso a la dirección. Con la aprobación de la dirección, el reclamo es canalizado a Sistemas de Información, u otra área funcional similar, para su implantación.

¿La compañía posee un procedimiento escrito para añadir, cambiar, y eliminar límites de control de acceso?

SI ❑ NO ❑

¿Los programadores de sistemas y aplicaciones tienen acceso a programas o data de producción?

SI ❑ NO ❑

¿Existen procedimientos que definan las funciones de visualizar, añadir, cambiar y eliminar data, y restringir el acceso de los individuos a únicamente la data o transacciones para que cuenten con una probada necesidad de conocer?

SI ❑ NO ❑

¿Cómo se otorgan y cambiar las contraseñas?

Las contraseñas deben ser otorgadas verbalmente, en persona, o por vía telefónica. También pueden ser otorgadas por medio del correo de la compañía o en sobres con la etiqueta "personal". El cambio de las contraseñas puede usualmente realizarse en línea. Sin embargo, algunos sistemas requieren que el individuo solicite el cambio de contraseña al área de Sistemas de Información, la que, a su tiempo, suministra la nueva contraseña. El otorgamiento de contraseñas y los cambios deben ser documentados en un formato escrito de procedimientos relativos a contraseñas.

¿La compañía posee procedimientos escritos para el cambio y otorgamiento de contraseñas?

SI ❑ NO ❑

¿La política de la compañía prohibe el intercambio de contraseñas?

SI ❑ NO ❑

¿Cuáles son las reglas para delimitar la longitud de la contraseña, la repetición de caracteres, y hacer la contraseña difícil de deducir?

Generalmente, las reglas aceptadas para construir contraseñas son que exista un mínimo de 6 caracteres alfanuméricos sin ningún vínculo común para su elaboración. Por ejemplo, las personas no deberían usar el mes, día y año de su nacimiento u otra información de ese tipo.

¿Las reglas para la creación de contraseñas están adecuadamente definidas?

SI ❑ NO ❑

¿Con qué frecuencia se cambian las contraseñas y como se evita la duplicación de las mismas?

Varios sistemas disponibles en la actualidad pueden ser seteados para solicitar cambios de contraseña con regularidad.

¿La compañía requiere de cambios frecuentes de contraseñas?

SI ❑ NO ❑

¿Se han establecido medidas para prevenir el despliegue de contraseñas durante el "logon", su impresión, o archivo bajo formas no encriptadas?

SI ❑ NO ❑

¿Están restringidos los usuarios a terminales específicas, tiempos en el día, y días de la semana donde así se requiera?

SI ❑ NO ❑

¿Los usuarios son automáticamente desconectados (logged-off) si permanecen inactivos durante un período específico de tiempo?

SI ❑ NO ❑

¿Las contraseñas y privilegios de ex-empleados son oportunamente cancelados?

SI ❑ NO ❑

¿Qué acciones se toman en el caso que un usuario es culpable de violaciones repetidas a la seguridad?

La compañía debe tener una política de violaciones a la seguridad. Las acciones pueden variar desde no hacer nada hasta emitir una carta de advertencia, una suspensión o el despido del empleado. La acción a tomar dependerá de la gravedad de la falta.

¿La compañía cuenta con una política de acción en caso de una violación a la seguridad del sistema?

SI ❑ NO ❑

¿Los reportes de violación y actividad de seguridad (log files) se revisan regularmente?

SI ❑ NO ❑

¿Se han establecido políticas y procedimientos para controlar el acceso a la data y para controlar el procesamiento concurrente de data?

SI ❑ NO ❑

¿La pantalla de inicio de sesión muestra una notificación de seguridad o un aviso de advertencia?

SI ❑ NO ❑

Puntaje: Anótese un punto por cada pregunta respondida con un "SI".

Puntaje total para los controles lógicos de acceso: 24

Puntaje de la evaluación: _____

CONCLUSIONES

- En la medida que los sistemas de información están logrando controlar un mayor nivel de información clave para los negocios, es de vital importancia para los mismos poner en practica una serie de controles que brinden la seguridad de un activo tan valioso como es la información del negocio, los sistemas que lo controlan y los mecanismos de acceso a los mismos.
- El desarrolllar una auditoría de sistemas en una base regular (por ejemplo: cada año), puede contribuir enormemente a mejorar los controles para proteger la información del negocio.
- Esta técnica de auditoría, a diferencia de la técnica de análisis de riesgo, esta basada en una investigación de la vulnerabilidad del activo a proteger, pudiendo este activo ser los sistemas de información o la información misma.
- Esta tecnica provee básicamente algunas direcciones claves, para identificar en donde los sistemas de información deben reforzar sus controles.

BIBLIOGRAFIA

- "The Service Management Audit"

  by Colin Armistead & Grahan R. Clark

  Published by Cranfield School of Management

- "The Computer Security and Fraud Prevention"

  by Kenneth Lindup & Lance Reeve

  Published by SRI International