LA SEGURIDAD Y CONFIABILIDAD DE LOS DATOS EN LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADA

Félix Armando Rivera León*
felix_arl@hotmail.com

RESUMEN

Una multiplicación rápida de los dispositivos del terminal y el crecimiento de los sistemas distribuidos añaden nuevas dimensiones a la tarea del auditor para asegurarse de tener un sistema seguro de PD. Aunque no es perfecto el sistema de comunicación de datos, varios conceptos de diseño y requisitos que los auditores deben entender para simplificar sus evaluaciones y para que puedan recomendaciones razonables.

Palabras clave: Sistemas de información, auditoría, informática.

ABSTRACT

A rapid multiplication of the terminal devices and the growth of distributed systems add new dimensions to the auditor task to ensure you have a safe system of PD. Although there is not perfect system of data communication, several design concepts and requirements that auditors should understand to simplify their assessments and to allow them reasonable recommendations.

Keywords: Information Systems, audit, computing:

* Doctor en Ciencias Contables y Empresariales – UNMSM, Magíster en Administración con mención en Gestión Empresarial. Contador Público Colegiado con 35 años de experiencia profesional. Profesor Principal de la Facultad de Ciencias Administrativas – UNMSM. Ha desempeñado diversos cargos administrativos en la facultad y en diferentes entidades del sector público y privado.

INTRODUCCIÓN

La seguridad y la confiabilidad son las consideraciones primordiales al hacer la auditoría de cualquier sistema de comunicaciones de datos. Su importancia aumenta según se amplían los límites del sistema total y según aumenta el valor y el volumen del tráfico de datos.

El auditor encontrará que los sistemas seguros y confiables sencillamente no existen. Por el contrario, evolucionan a través de una serie de consideraciones en cada componente del sistema durante su diseño, su implantación, y su operación. Hoy en día es más probable que se incluya a los auditores en las etapas de diseño de los sistemas de comunicaciones de datos, en vez de convocarlos en las etapas del diseño del desarrollo de las aplicaciones. Esto se debe a que los sistemas de comunicaciones de datos son relativamente nuevos y más sujetos a cambios, permitiéndoles así una participación más activa durante las consideraciones del diseño.

Los sistemas tradicionales comerciales de comunicación de datos se desarrollan según la premisa básica de que operarán en un ambiente "amistoso". En tales casos, el diseño y la programación de los sistemas se realizan por los métodos de reaccionar ante situaciones provocadas por el error humano, el mal funcionamiento del equipo, o el diseño defectuoso de los programas operacionales. Estos factores son válidos y deben considerarse al diseñar y revisar un sistema de comunicaciones de datos, pero el auditor también debe suponer que existirá un ambiente "hostil" en donde la amenaza de una deliberada intrusión se considera como factor normal. Las revisiones de auditoría deben enfocar al sistema tanto desde el punto de vista "amistoso" como desde el punto de vista "hostil".

Los tópicos de la seguridad y la confiabilidad presentan múltiples facetas y van desde la estructura de la organización total hasta la selección de los recursos humanos y de equipo. En esto debemos destacar las áreas significantes que deben considerarse para alcanzar el grado de seguridad y confiabilidad necesario para garantizar el nivel y la clase de servicio requerido. Estas áreas se consideran con relación al desarrollo de los sistemas como a su operación cotidiana.

ANÁLISIS

Un sistema de comunicaciones seguro se define como un sistema automatizado en que una transacción (mensaje) que ha entrado por una estación de entrada (originador) será:

- Siempre entregado a la estación de salida correcta (receptor).
- Con el mismo contenido con que se le dio entrada.
- Sin ninguna posibilidad de que ninguna persona no autorizada pueda enterarse de la transacción ni demorarla durante la transmisión.

En todos los casos, es necesario establecer la autorización para el originador y el receptor tanto respecto al tipo de transacción como respecto a la estación de origen o receptora de esa transacción. Consiguientemente, una violación de seguridad se define como una infracción a la red global entre el originador y el receptor, mediante la cual alguien ha tenido acceso al mensaje para el propósito de su observación no autorizada, su aceleración, su cambio, o su modificación, o ha podido introducir o sacar datos de la red.

En realidad, un sistema totalmente seguro es inalcanzable, pero es posible proporcionar niveles adecuados de seguridad, de acuerdo con los riesgos involucrados y dentro de las limitaciones impuestas por el personal y los recursos físicos, tecnológicos y financieros de un ambiente real.

Un sistema adecuadamente seguro necesariamente depende del logro de un nivel adecuado de confiabilidad o de apresto operacional. El vocablo "confiabilidad" implica un sentido más amplio que su definición técnica normal y es, esencialmente, equivalente al concepto del apresto operacional. Así, "confiabilidad" se refiere no tan solo al continuo estatus operacional de las computadoras, otros equipos y programas, sino también al "sistema" como entidad, considerando incluso al personal, los procedimientos, los requerimientos de logística, y la facilidad con que se puede hacer el mantenimiento.

Las metas de un sistema seguro y confiable son las siguientes:

- Un mensaje aceptado por el sistema jamás se perderá, será distorsionado, ni duplicado, acelerado, ni retrasado sin autorización.
- El sistema jamás estará completamente fuera de servicio, aunque el servicio que ofrece ocasionalmente puede ser más bajo de lo normal.
- La falla de un solo nódulo o paso de transmisiones no aislará a ningún punto de la red de cualquier otro punto.

- Cualquier error en la transmisión del mensaje, su recepción, el formato de su contenido, o su procesamiento será detectado y provocará la rápida notificación al personal de operaciones que es responsable del sistema.

Para obtener el apresto operacional de las redes de comunicaciones primero es necesario determinar el nivel necesario de confiabilidad del equipo y, a la inversa, la cantidad y el grado de las fallas que pueden permitirse sin arriesgar los objetivos del sistema global. Una vez que esto ha sido determinado, entonces le corresponde al planificador del sistema diseñar la red y sus componentes para alcanzar las metas especificadas.

La protección total que ofrezca un sistema "seguro" no es una función de los niveles acumulativos de la seguridad de todos los puntos en la transferencia de datos o mensajes sino que, a la inversa, está relacionada con el nivel que haya en cada punto de la posición. Este nivel de exposición a las violaciones de seguridad disminuye según los datos progresan desde un punto de entrada hacia el punto de intercambio nacional. Esta disminución en exposición se debe a varios factores, que incluyen:

- La transferencia de datos del procesamiento manual al procesamiento automático.
- Un aumento en la complejidad de los medios y los procedimientos de transmisión junto con un correspondiente aumento en los controles.
- Una concientización de la administración de los puntos de intercambio y los conmutadores centrales en cuanto a la importancia de la seguridad, aumentando así su compromiso de asegurarla

Aunque el riesgo de la exposición a una violación de seguridad disminuye según el tráfico fluye de las estaciones individuales hacia su destino final y se concentra en el engranaje de los datos, la gravedad de una violación o del mal funcionamiento del sistema, aumenta. A pesar de que la transmisión de mensajes no autorizados desde un punto terminal es grave, ésta puede ser un problema menor al compararla con la interrupción del servicio en algún punto de intercambio local o en algún centro nacional de conmutación. Una grave violación de seguridad o una grave falla del sistema en algún concentrador o conmutador dentro de la red pudiera tener consecuencias gravísimas.

El desarrollo de normas de confiabilidad y seguridad es esencial para el funcionamiento de cualquier sistema de comunicaciones. Basándose en la cantidad potencia de nódulos y en el hecho de que éstos pudieran representar entidades independientes que crucen a través de muchos límites organizacionales, la vigilancia del cumplimiento de las normas a través de una red total se vuelve extremadamente compleja. Por lo tanto, sería mejor adoptar y hacer cumplir normas para cada uno de tres grupos distintos:

- Puntos de servicio local (v.gr., operador, terminal, oficina).
- Puntos de intercambio con otros puntos y con la red central (punto de concentración de la red).
- Puntos de intercambio entre la red y otras redes (oficina central de la red, punto de intercambio nacional).

En combinación con esto, es necesario establecer salvaguardias legales adecuadas para proteger a los integrantes de la red respecto a los problemas que pudieran suceder por fuera del alcance de sus responsabilidades y jurisdicciones, como por ejemplo, la entrada de datos no autorizados a la red.

El tema de la seguridad y confiabilidad de los sistemas de comunicaciones de datos se puede analizar desde dos puntos de vista. El primero tiene que ver con los requerimientos que deben imponerse durante el diseño y la implantación del sistema, y el segundo, tiene que ver con los requerimientos cotidianos de seguridad y confiabilidad necesarios para garantizar la operación segura del sistema.

A cada nivel de diseño e implementación del sistema de comunicaciones es necesario considerar varios factores para asegurar niveles adecuados de seguridad y confiabilidad. Estos factores incluyen los requerimientos del sistema, las partes que componen al sistema, los mensajes (datos), y las medidas de contabilidad y reconciliación. Todos tienen diferentes grados de interés para el auditor del proceso de datos.

Existen cuatro categorías básicas de requerimientos de seguridad en un ambiente de comunicaciones. Estas tienen que ver con el acceso a la red, el costo de la seguridad, la detección de las intrusiones, y el personal:

- **Prevención del acceso físico al lugar.** La precaución más obvia que se puede tomar para establecer un ambiente seguro es la prevención del acceso no autorizado a la instalación o a los componentes del sistema. En el caso de los sistemas de comunicaciones, esto pudiera significar acceso a un terminal de entradas o de salidas, a cualquiera de las líneas de comunicaciones y los puntos de intercambio, y al (los) centro (s) de computadores y los archivos de almacenaje de datos. En el caso del centro de computadoras, la prevención seguiría los patrones normales que existen en cualquier ambiente restringido e incluyen:
  - Vigilancia.
  - Facilidades de entrada restringida, laberintos.
  - Pases, investigaciones de identidad, máquinas de huellas digitales, y similares.
  - Cerraduras de puertas de tipo de identificación o de combinaciones.

  Estos artículos generalmente forman parte de la tarea de la planificación de la planta física.

  Las medidas de seguridad requeridas para proteger los datos almacenados comienzan con la limitación del acceso físico e incluyen hasta la facilidad de almacenaje. Esta debería estar físicamente separada de las computadoras para disminuir su vulnerabilidad a los incendios y otros peligros. Los archivos deberían protegerse de la interferencia magnética mediante la instalación de escudos entre la facilidad de almacenaje y las áreas públicas o desprovistas de protección. Como el daño ocurriría solamente si los archivos están cerca de la fuente del campo, es posible que solo sea necesario ubicar las unidades de almacenaje lejos de las paredes externas.

  La interferencia de las frecuencias de radio también puede causar problemas. Las causas pueden ser intencionales o accidentales si el centro de computadoras está ubicado cerca de transmisores de radar de alta potencia o de líneas eléctricas de alto voltaje. Sus efectos pueden producir fallas en las computadoras y en las comunicaciones. Una planificación adecuada de los sitios y las redes contribuirá a evitar problemas, pero en algunos casos puede ser necesario construir escudos.

  El acceso a las facilidades de trasmisión es más difícil de evitar porque, por su propia naturaleza, quedan fuera del ambiente protegido del terminal o de la central de computadoras. Aún en las redes privadas arrendadas, las rutas de transmisión de mensajes pueden incluir líneas públicas durante alguna parte de su trayectoria. Esto significa que en algún punto entran y salen con alguna facilidad de carga común y en ese punto, entre otros, son susceptibles a la intrusión. Como consecuencia, se necesitan otros métodos para evitar la observación no autorizada de los datos que se transmiten por las líneas de comunicaciones. Estos pueden incluir el diseño de características protectoras para cada mensaje al igual que la codificación de las transmisiones para que los datos sean inservibles para el intruso.

- **Prevención del acceso operacional al sistema.** Si se logra el acceso físico a la instalación, el próximo nivel de seguridad tiene que ser la prevención del acceso operacional al sistema. Las características de seguridad a considerarse durante el diseño de la red de estaciones remotas deberían incluir:
  - Terminales controlados por computador.
  - Estrictos procedimientos de “log-in” y ‘log out”.
  - Verificación de la entidad del operador del terminal mediante la computadora.
  - Control de los mensajes de entrada y salida (numeración en secuencia)

  Si se logra el acceso a la computadora principal o al centro de control, el segundo nivel de salvaguardias a vencerse debería incluir:
  - La separación física del control de la computadora y el control de la red.
  - Contraseñas para que el operador logre acceso la computadora.
  - Restricciones en cuanto a los tipos de datos que pueden enviarse o recibirse por los centros de control.

  El acceso operacional a los datos almacenados pudiera restringirse mediante el uso de teclas y protección del archivo de contraseñas para las cintas y los discos. En algunos casos, los datos también pudieran codificarse para proteger su privacidad.

Los dos propósitos principales de la observación de un sistema son la búsqueda de una o varias transacciones particulares, y la recopilación de datos sobre la operación global, el volumen, las estadísticas financieras; los datos sensitivos, y cosas por el estilo. Tales datos operacionales o financieros generalmente estarán disponibles más tarde –compaginados, analizados y listos para usarse-. La observación de las líneas con el propósito de acumular datos crudos sería más difícil que su obtención por otros modos, tales como a través del personal que tenga acceso a los datos en su forma final, y organizada.

La búsqueda de un mensaje específico es una razón viable para observar una línea. Aquí la protección está para hacer que los datos sean inservibles en su formato observado, o para hacer que el uso del equipo de observación no sea económico al compararlo con otros métodos que pudieran vencerse con mayor facilidad. La ruta de transmisión de los datos esencialmente no está protegida fuera del restringido ambiente físico del centro de intercambio, y es vulnerable a la observación en cualquier punto. Por lo tanto, suponiendo que un intruso pudiera lograr acceso a las líneas de transmisión, es necesario proporcionar protección básica para los datos mismos. Las consideraciones del diseño deberían incluir:

– Codificación de los mensajes.
– Líneas de trasmisión múltiple.
– Uso de flujos de datos sincrónicos y continuos.
– Uso de las facilidades de transmisión de mayor velocidad factibles o disponibles.
– Uso de rutas alternas y configuraciones de líneas rotativas.

Entre todos, la codificación de los datos proporciona el más alto nivel de seguridad y se ha empleado exitosamente por varios años. Hay que hacer concesiones entre el uso de los dispositivos físicos de hardware en cada línea, los programas criptográficos en los computadores, o las combinaciones entre ambas. Es necesario examinar cada uno según el verdadero nivel de seguridad que se requiere.

Las demás salvaguardias mencionadas son más fáciles de vencer que la codificación; sin embargo, reducen las posibilidades de la observación accidental, o la búsqueda casual de los datos que se están transmitiendo porque requieren un mayor grado de complejidad en el equipo y las técnicas que se deben usar. Por lo tanto, aunque su propósito principal puede basarse en razonamientos técnicos y económicos, el tipo y el uso de las líneas y procedimientos de comunicaciones tiene algo que ver en el mantenimiento de la seguridad y el apresto operacional de la red.

Muchos de los factores que influyen en las características de seguridad y confiabilidad de las comunicaciones forman parte del diseño de los mensajes que pasan por el sistema. Los requerimientos del diseño deben comenzar con la selección de un juego estándar de códigos que sea adecuado con paridad de caracteres.

El proceso de autorización debería incluir las comprobaciones y aprobaciones necesarias, antes que los mensajes entren al sistema. Se debe considerar esta preparación como parte del programa total para la seguridad del sistema. A estas alturas, un mensaje autorizado, en formato legible por la máquina, se le presenta al sistema para su transmisión.

El diseño del sistema tiene que incluir por lo menos los siguientes pasos en el proceso de autorización:

– Validación del terminal originador respecto a la propiedad, la estación correcta dentro de la línea, etc.
– Comprobación de que la estación está autorizada para transmitir en ese momento específico.
– Confirmación de la señal de entrada del operador y validación del formato del mensaje
– Verificación de la autoridad del operador (la estación) para transmitir ese tipo de mensaje
– Validación de la secuencia de numeración del mensaje.
– Prueba de los códigos correctos de autorización que se encuentran incorporados en el mensaje

Los procedimientos a seguirse en caso de que un mensaje no pase todos los pasos de autorización también deben considerarse durante el diseño del sistema. Dependiendo de

la gravedad o la frecuencia con que suceden, deberían ser los siguientes:

– Rechazar el mensaje.
– Rechazar el mensaje y notificarle al supervisor.
– Desconectar la línea y evitar otras transmisiones por ella.
– Cambiar la línea a estatus de monitor solamente, suspender el procesamiento del mensaje, y avisarle al supervisor.

Puesto que cualquier error detectado por el sistema puede formar parte de un patrón que pudiera sugerir un intento de violar la seguridad del sistema, es imperativo que el diseño incluya la capacidad de detectar y anotar cualquier incidente.

Cuando las pruebas preliminares indican que un originador autorizado ha dado entrada a un mensaje dentro del sistema, los procedimientos de segundo nivel que deben cubrirse durante la etapa de diseño son los parámetros para la validación de los mensajes. Tales especificaciones de formato y contenido de los mensajes deben estandarizarse y cumplirse fielmente para que el sistema pueda funcionar.

Las pruebas mínimas para la validez de los mensajes son:

– Edición de las posiciones en cuanto a la corrección de los caracteres de control, campos de direccionamiento y de datos, y limitaciones de líneas y de formatos.
– Validación de los datos en cuanto a números de encaminamiento, direcciones, tipos de códigos, e información de contenido específico orientada respecto a un usuario específico.
– Pruebas de autorización para los datos codificados, las palabras de prueba, y otros tipos de pruebas relacionadas con la seguridad, tales como los campos múltiples de unidades monetarias idénticas.

El proceso de validación sirve para varios propósitos: aumenta el nivel de seguridad del sistema, ayuda a asegurarse de que los datos necesarios para el procesamiento de entrega sean válidos, y proporciona el momento oportuno dentro del ciclo de procesamiento para capturar datos respecto al control de los mensajes. Una vez que el mensaje se ha validado, el diseño debería incluir la devolución de un indicio de aceptación positiva del mensaje para el originador.

Hay varios factores involucrados en la entrega de los mensajes de modo que lleguen únicamente a su propuesto recibidor:

– Se verifica el encaminamiento del mensaje buscando su validez y autenticación.
– No se hace observación de líneas que no estén autorizadas: si se hace, los datos observados serán inútiles.
– Todos los mensajes se han entregado y se han contabilizado.
– El mensaje no se ha alterado, duplicado, acelerado, o demorado.

Los procedimientos de verificación de encaminamiento deberían diseñarse para asegurar que:

– El destino es un punto válido dentro de la red.
– El destino está autorizado para recibir el tipo de tráfico en cuestión.
– Se hace una conexión positiva con la estación y se le valida antes y después de la transmisión del mensaje.
– Se recibe notificación de la aceptación del mensaje por parte del terminal a la entrega, con la identificación del terminal incluido en el acuse de recibo.
– Se transmiten números de salida continuos y seguidos como parte del mensaje.
– Se mantiene un registro histórico de todos los mensajes transmitidos.
– Los algoritmos de activación y de encaminamiento, proporcional el eficaz procesamiento del tráfico, para evitar los retrasos innecesarios en los mensajes en tránsito.

Un aspecto adicional de garantizar la seguridad del sistema incluiría el diseño de facilidades para producir pruebas de la entrega.

El uso de los Números de Referencias especiales es un importante aspecto de la protección e identificación de los mensajes, pero estos no capacitan a un nódulo receptor de una red para que sepa si ha recibido todos los mensajes que

se le han dirigido dentro de un período de tiempo lo suficientemente corto como para permitir una posible acción. La pérdida de un mensaje indudablemente se descubrirá días más tarde posiblemente, en el transcurso de las actividades o de la contabilidad, pero no será mediante los procedimientos de comunicaciones.

Para llenar este vacío, la estación transmisora debería hacer la entrada de un número de serie en secuencia según el recibidor, junto con el mensaje. Si un número más alto se recibiere fuera de secuencia, el recibidor sabría cuántos mensajes esperar. Aunque pudiera ser engorroso, alertaría al operador en cuanto al tipo de falla si un conmutador de computadora recibe mensajes y no los retransmite a su vez. Las pruebas normales de control de línea y de secuencia no detectan este tipo de acontecimiento. Tal validación de secuencias en el punto de recibo se puede llevar a cabo en línea, o al final del día como parte de los procedimientos normales del cierre de actividades.

En el ambiente de comunicaciones existe muy poca o quizás ninguna verdadera protección contra la observación no autorizada de las líneas, de las redes; por lo tanto, para proporcionar el grado de seguridad necesario, el diseño del sistema necesita incluir varios modos para proteger los datos que el mismo mensaje contiene. El uso de los dispositivos y proceso de codificación en distintos puntos del sistema, o de palabras en código dentro del mensaje, reduce la posibilidad de la modificación no autorizada de los mensajes. La transmisión de los mensajes por sistema múltiplex junto con otros, aumenta la dificultad de observación.

En un "ambiente ideal" en que las líneas estén libres de interferencia, otro enfoque sería proporcionar un alto nivel de observación de las líneas del sistema para detectar los errores causados por intrusos potenciales. Tal capacidad de detección da aviso temprano de la conexión de dispositivos de observación o intercepción dentro de la red. Estas conexiones alteran la sincronización de las transmisiones y causan errores.

Una de las reglas cardinales que hay que seguir al diseñar sistemas de comunicaciones es la de garantizar la contabilidad de los mensajes. Esto significa que una vez que el sistema ha aceptado un mensaje, este se entregaría al recibidor correcto según se aceptó. Ningún mensaje jamás se perderá, se demorará indebidamente, ni se acelerará. Para garantizar este requerimiento, el sistema tiene que diseñarse de modo que cada mensaje se almacene seguramente en algún dispositivo permanente, del cual se le pueda reintegrar al sistema activo cuando sea necesario. Las copias múltiples de los mensajes tienen que almacenarse para garantizar la contabilidad en caso de la falla de un dispositivo. En los ambientes de multicentros puede ser aconsejable retener copias de todo el tráfico en todos los centros. Es necesario diseñar controles internos para el sistema mediante sistemas de numeración u otros mecanismos internos de direccionamiento, para permitir la recuperación de los datos del mensaje según sea necesario. Estos controles deben contener datos de pista de auditoría, los que deben incluir, por lo menos:

- Estación de entrada y salida, identificación de la línea, y número de secuencia.
- Fecha y hora de la entrega.
- Cantidad de copias entregadas.
- Estatus del mensaje (normal, duplicado, etc.).

El diseño del sistema debe requerir la positiva aceptación o el rechazo de todos los mensajes.

La estación receptora debería proporcionar confirmación de la identificación antes y después de la entrega de un mensaje, y debería acusar recibo de la entrega automáticamente. Por lo menos cada 24 horas, los archivos del sistema de conmutación deberían verificarse respecto al tráfico del día anterior; para lograr esto, es necesario diseñar el sistema de modo que contenga mecanismos de envejecimiento de los archivos.

Los programas de recuperación del sistema deben diseñarse de modo que rindan cuenta por todos los mensajes en tránsito después de una falla. También deben ser capaces de restaurar el archivo de mensajes activos y, de continuar el servicio sin alterar la prioridad de los mensajes. Los programas de recuperación deben diseñarse de modo que solamente las personas autorizadas logren acceso a los mensajes entregados. Los mensajes recuperados deberían identificarse claramente para indicar que no son originales, y esto debería ser independiente de cualquiera de los procesos de contabilidad.

RECOMENDACIÓN

Las implicancias de la seguridad y la confiabilidad en un sistema de comunicación de datos son amplias. Evidentemente, mientras más amplio sea el alcance del sistema, más interesante será la tarea de evaluación que corresponda al auditor. Es recomendable desarrollar una serie de procedimientos de comprobación para realizar los análisis detallados del sistema en evaluación.

LITERATURA CITADA

Carlo Barco Gómez (1985). *Introducción al proceso de datos para los negocios.* Editorial Mc. Graw Hill, Bogotá.

Adriana Gutierrez (1998). *Guía International Federation of Accountants.* Editorial, Auto edición: Adriana; ciudad, Mexico.

Unidad Educativa Técnica "Luis Felipe Borja del Alcázar",1999. *Enciclopedia Práctica de la Informática.* Editorial Cinco SA., Colombia.

Detmer W. Strub Yr.; Rosann Webb Collins, 1990 *Information System in Managent.* Editorial Reston Publishing Company, Inc., Virginia.

Davis, Gordon B. 1972, *La auditoría y el procesamiento electrónico de información*; Instituto Mexicano de Contadores Públicos , A C ; México

Detmer W. Strub Yr.; Rosann Webb Collins, 1990 American Intitute of Certified Public Accountants, California.

Piattini, Mario G. y De Peso, Emilio. (1998). *Auditoría en informática, un enfoque práctico.* Editorial Ra-Ma, México.