UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

SISTEMAS DE SEGURIDAD EN LOS CENTROS DE COMPUTO

SEMINARIO DE INVESTIGACION ADMINISTRATIVA

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN ADMINISTRACION

P R E S E N T A :

ALEJANDRA DIANA CONTRERAS MARTINEZ

Director del Seminario:

Lic. Manuel Osuna y Fernández

1 9 8 1

I N D I C E

Página

Página

I N T R O D U C C I O N

Siendo el objetivo de la información el proveer elementos de juicio a los niveles decisorios, la función de un sistema de computación de datos será la de coadyuvar al proceso de toma de decisiones, proveyendo información correcta y oportuna.

En cada uno de los pasos del proceso administrativo, un sistema de computación de datos puede asumir un rol muy importante. Su función básica será la de constituirse en el centro de gravedad del sistema de información directiva, incluyendo en este sentido, la capacidad de controlar su propia información.

El tratamiento de la información parece, a menudo, más difícil de lo que en realidad y probablemente sea, debido a la falta de control. En el mejor de los casos, tiene el directivo un sentido bastante oscuro. Toda institución requiere de información convenientemente tratada, que le permita reducir el grado de incertidumbre en la toma de decisiones y que sea un auténtico apoyo para la gestión de los directivos.

Por tanto, la información que reciba cada directivo debe de tener la seguridad necesaria para que se logre una marcha correcta del área de la empresa bajo su ámbito de responsabilidad y asimismo, controlarla de la mejor manera.

Ahora bien, para que se pueda ejercer un mejor control en los sistemas de computación de datos utilizados en las diferentes instituciones, es necesario contar con Sistemas de Seguridad que se hayan planeado y adecuado correctamente, evitando con ésto alguna desviación o falla que surjan posteriormente.

En el Capítulo I, se define lo que son los Sistemas de Seguridad, asimismo, se trata a grandes rasgos aquellos sistemas que emplean las tiendas comerciales para proteger sus mercancías contra robo, y la seguridad industrial tan esencial para cualquier organización.

El Capítulo II, "Sistemas de Seguridad en los Centros de Cómputo", se encuentra desglosado de la siguiente manera:

Primeramente, se describe la división de responsabilidades en este aspecto de la seguridad para un mejor control y poder alcanzar los objetivos que se fijen en el sistema de seguridad, tanto física como lógicamente. También, se hace mención del posible costo que pueda tener la seguridad lógica.

En segundo término, se hace mencion de los Controles de Seguridad para la Exactitud de la Información, en el cual se enuncian algunas pruebas de aspecto general que se deben aplicar a la información, tanto de entrada como de salida, así como algunos de los que se pueden aplicar, de acuerdo al sistema de procesamiento, ya sea en Lotes, Tiempo --

Real o por Teleproceso. Se mencionan también, algunos de los procedi-- mientos a aplicar para recuperarse cuando ocurra una falla en el equipo y en la información.

En tercer lugar, se ve el aspecto de la privacidad de la información; en esta parte se hace mención a las restricciones y autorizacio-- nes para poder acudir a la información que se maneja en toda institu- - ción pública, por medio de tablas de autorización.

Por último, se trata la Seguridad Física. Aquí se describe la -- ubicación física que debe tener toda Unidad de Informática, así - - -- como las precauciones que se deben tomar contra fuego, robo y sabotaje.

El Capítulo III, "Análisis de los Sistemas de Seguridad en el --- Sector Público Central", se describe el desarrollo de una encuesta realizada en 15 Unidades de Informática, para estar en posibilidades de poder comprobar o disprobar la hipótesis planteada "Si se aplican las medidas de Seguridad en los Centros de Cómputo del Sector Público Central en un 80%".

Por último, en el Capítulo IV, se presentan las conclusiones y algunas recomendaciones para las Unidades de Informática que integran el Sector Público Central.

C A P I T U L O I

CONCEPTO SOBRE SISTEMAS DE SEGURIDAD

1. Definición de Sistemas de Seguridad

Existe una gran cantidad de tratados que hablan sobre sistemas. - El término tiene significados reservados en todas las disciplinas y campos de investigación, se habla de sistemas educativos, sistemas de - -- transporte, sistemas de información, sistemas sociales, sistema humano, sistemas de seguridad, etc., existiendo por lo tanto, gran variedad de definiciones de este concepto, algunas muy sencillas y otras muy complicadas, pero todas llegan prácticamente a la misma. En el presente documento sólo trataré los sistemas de seguridad.

Murdick G., Robert y Ross E. Joel [1], nos define el sistema de - la siguiente manera: "Serie de elementos unidos de algún modo, a fin de lograr metas comunes y mutuas".

---

[1] Murdick G., Robert y Ross E. Joel, Sistemas de Información Basados - en Computadoras para la Administración Moderna, México, Ed. Diana, - 1974, Pág. 27.

Partiendo de esta sencilla pero completa definición se puede decir que un sistema de seguridad es EL CONJUNTO DE MEDIDAS TECNICAS DESTINADAS A CONSERVAR LA SALUD, LA VIDA Y LA INTEGRIDAD FISICA DEL HOMBRE Y TENDIENTES A CONSERVAR LOS MATERIALES, EQUIPOS E INSTALACIONES.

Dentro de los sistemas de seguridad, se pueden incluir aquellos que emplean las tiendas comerciales para proteger sus mercancías contra robo, el sistema de seguridad industrial y el sistema de seguridad en los centros de cómputo; en la siguiente sección trataré brevemente los dos primeros sistemas y posteriormente se hará una descripción detallada del tercero.

I.I Sistemas de Seguridad Existentes en el Mercado Mexicano

Los sistemas de seguridad que emplean las tiendas comerciales para proteger sus mercancías contra robo, varía entre una y otra, según sean sus necesidades y presupuesto asignado a este concepto.

Así, se tiene por ejemplo, que una de las tiendas comerciales más importantes de la ciudad de México no emplea ninguna medida técnica para proteger sus mercancías, su sistema consiste en emplear vigilantes vestidos de civiles distribuidos por toda la tienda, a su vez los empleados avisan a éstos en caso de existir alguna anomalía. No existen cajas registradoras, los pagos son efectuados a las cajeras, las cuales cuentan con un cajón para guardar el dinero. Esta cajera no tiene con-

tacto directo con la mercancía, ésta es entregada por la vendedora a -- otra persona que se encargará de entregarla directamente al cliente, -- previa presentación de su nota de pago. Por lo tanto, si un empleado - quisiera sustraer mercancía, tiene que estar de acuerdo con las otras - dos personas que intervienen en la operación de venta.

No existen alarmas contra intrusos en puertas, aparadores y ventanas, éstos son vigilados por los policías o veladores.

Dicha compañía ha declarado que sus pérdidas son mínimas por concepto de mermas o pérdidas de mercancía.

Otras compañías emplean métodos más modernos, colocan a sus ar- - tículos una etiqueta sensibilizada. Esta etiqueta es difícil de remover por un ladrón, pero muy fácil para la tienda.

A la salida de cada Departamento o en las salidas de la tienda, - se colocan dos pedestales (columnas), que funcionan a través de una señal de alta frecuencia, la cual detectará la entrada y salida de etiquetas (aun cuando sea transportada en un portafolio) entre sus campos de acción.

Cuando una etiqueta es detectada dentro del campo de acción de -- los pedestales, suena la alarma, ya sea a través de un sonido audible - o una señal visual. La alarma puede estar localizada cerca de los pe--

destales o bien, en algún lugar clave para su mejor control.

La etiqueta es removida en la caja de pago antes de que llegue al campo detector.

A ésto se auna el hecho de colocar alarmas en puertas, aparadores y ventanas, así como ser reforzada por vigilantes, el sistema brinda -- una mayor protección, que se ve reflejada en los decrementos de pérdi-- das por este concepto.

Otro sistema utilizado en tiendas comerciales es el circuito ce-- rrado de televisión.

Las cámaras de televisión son colocadas en localidades estratégi- cas y producen una imagen en una pantalla en el puesto del vigilante. - La cámara va recorriendo todas las áreas de la tienda, cuando se detec- ta alguna anomalía, el vigilante de la cámara hace una llamada telefóni_ ca al vigilante que se encuentra en la puerta de salida de la tienda y_ le proporciona las características de la persona que pretende sustraer_ la mercancía, para que ésta sea detenida.

Este sistema también es suplementado con alarmas contra intrusos_ que se colocan en puertas, aparadores y ventanas.

1.2 Seguridad Industrial

Otro de los sistemas de seguridad existentes en el mercado mexicano es la seguridad industrial, este tema es tan extenso que su desarrollo se llevaría otro documento sumamente extenso, con lo cual sólo trataré en forma muy breve los puntos más relevantes.

Lazo Cerna, Humberto [2], define la seguridad industrial como sigue: "Conjunto de conocimientos para evitar accidentes en el trabajo", o sea que son todas aquellas medidas técnicas que se deben acatar en una empresa como parte de un programa de seguridad, para brindar protección a los empleados y además todas aquellas acciones para conservar en buen estado los materiales y equipos.

La seguridad industrial surge con el propósito de evitar los accidentes de trabajo dentro de la empresa.

Para tal efecto existen ciertas medidas de seguridad que ayudan considerablemente a reducir el número de accidentes de trabajo, entre éstos se encuentran los siguientes:

---

[2] Lazo Cerna, Humberto. Higiene y Seguridad Industrial. México, Ed. Porrua, 1973, Pág. 16

EQUIPOS DE SEGURIDAD PERSONAL.- Son las prendas de vestir normales hasta los accesorios que sobre las mismas se colocan los trabajadores, tales como anteojos, guantes y caretas.

PROTECCION DE LA MAQUINARIA.- Estas tienen por objeto librar a los obreros y empleados contra riesgos potenciales o latentes que encierran las máquinas.

PROTECCIONES ACCESORIAS.- Entre éstas se encuentran los espejos de vuelta cierga, flechas de tránsito, redes de contención, lubricación automática, herramientas especiales, lubricación automática y regaderas de emergencia.

También existen protecciones específicas para las personas que tienen contacto con la energía eléctrica, tal es el caso de las gafas, zapatos con suela de hule y sin clavos, guantes de hule impermeables, así como usar herramientas cuya punta o mago sean malos conductores de electricidad, etc.

Algunas de las medidas más importantes y que deben ser consideradas en todo tipo de empresas y hasta en el hogar mismo, son aquellas contra incendio, teniendo presente el giro de la empresa, se elegirán las más convenientes acorde a sus necesidades, a continuación enuncio algunas de estas medidas:

- Interrumpir la energía eléctrica al centro de trabajo incendiado, ya que si se emplea el agua como principal elemento, se pueden producir cortos circuitos, y provocar electrocutaciones.

- Contar con extinguidores de fuego, los cuales son muy variados, todo depende de lo que se esté incendiado y del material cercano a éste, así tenemos extinguidores de espuma, tetracloruro de carbono, de bióxido de carbono, extinguidores a base de sosa y ácido.

- Las tomas de agua para los bomberos deben de estar en lugares accesibles.

- Esto se puede reforzar con equipos y materiales auxiliares, tales como hachas, palas, carretillas, depósitos de arena, escaleras y mantas incombustibles.

Los detectores de fuego o de humo y las alarmas proporcionan gran ayuda para hacer frente a la situación.

De nada nos servirá el contar con buenos equipos preventivos si el obrero o empleado no sabe utilizarlos, por tal motivo, es de vital importancia proporcionarles entrenamiento e instructivos sobre el manejo de todos aquellos útiles y aparatos que deben utilizar para proteger

se de las actividades peligrosas que desarrollan, asimismo, deberán recibir instrucciones sobre las acciones a realizar en caso de emergencia, ésto se puede complementar con conferencias, carteles, películas, concursos sobre seguridad, boletines, periódicos, estadísticas y gráficas.

El servicio médico para los trabajadores es indispensable en cualquier organización. Si ésta es muy pequeña y con pocos riesgos, al menos se hace necesario un botiquín de primeros auxilios.

Los programas de seguridad son muy variados, pero debe de haber una pauta mínima en todos los casos, ésto depende del giro de la empresa, no es el mismo para un comercio, una fábrica de zapatos, para una fundición de metales, una mina o un hospital. El programa de seguridad debe tomar en consideración todos los siniestros potenciales, los que no están asegurados y los que están. Se prepara por la Dirección o Gerencia, quien debe tener la seguridad de que la planta y su personal no sufran daños por accidentes. Se preocupará de que haya protección contra todas las fuerzas causantes de deterioro o destrucción; incendios, explosiones, viento, inundaciones, averías en los equipos, accidentes del personal, a todo lo que pueda afectar a todos los activos productivos, a los beneficios y a lo que es más importante, el personal.

En México, la seguridad e higiene industrial, se encuentra regulada por el Reglamento General de Seguridad e Higiene en el Trabajo, el cual se encuentra fundamentado en los artículos 5, 132, 134, 330, 352,

423, 504, 509, 511, 512, 512-A, 512-B, 512-C. 512-D. 512-E, 523, 526, - 527, 527-A, 529, 540, 541, 876, 878, 885, 886, 887, 888 y 889 de la Ley Federal del Trabajo, en lo que se refiere a Seguridad e Higiene de los_ trabajadores; 101 y 105 del Código Sanitario de los Estados Unidos Mexicanos, así como en los artículos 88 y 89 de la Ley del Seguro Social, publicado en el Diario Oficial de la Federación del lunes 5 de junio de 1978.

C A P I T U L O II

SISTEMAS DE SEGURIDAD EN LOS CENTROS DE COMPUTO

2. ¿Quién debe ser el Responsable del Sistema?

El primer paso en el procedimiento para el diseño de los contro-- les necesarios de seguridad de un sistema de computación, es establecer quiénes serán los responsables de esta seguridad.

Para ésto es necesario que el nivel directivo más alto establezca qué tan estrecha quiere que sea ésta.

Una vez establecido el nivel de protección necesario, éste debe - ser incluido en todas las fases del sistema. Al igual que todos los -- aspectos del sistema de computación, el de seguridad debe de estar bien balanceado, es menester que todas las medidas de este sistema no dejen_ alguna parte desde la cual se pueda causar daño. Se puede poner espe-- cial atención al trabajo de los analistas o al de los operadores y des-

cuidarse el de los programadores y viceversa.

Por el hecho de manejar la información vital para la institución, la Unidad de Informática puede ser el blanco de ataque para poder obtener información o simplemente con el objeto de causar problemas. Para evitar ésto, es necesario que la Unidad de Informática implante un sistema de seguridad para proteger a la institución, al personal y a la información.

Este sistema de seguridad debe contemplar las medidas necesarias para evitar, en lo posible, el daño por fuego, inundaciones, sabotajes, errores de programación, de operación, etc., y todas y cada una de - -- aquellas que se crean pertinentes para lograr el nivel de seguridad deseado.

Para que se pueda cumplir con todas las medidas implantadas, es necesario nombrar personal que sea responsable de comprobar que todas ellas se lleven a cabo.

Estas medidas se pueden dividir en dos grandes áreas: la responsabilidad de las técnicas y los procedimientos de seguridad y la responsabilidad de las operaciones, una vez implantadas esas técnicas y esos procedimientos.

En ambas áreas la responsabilidad total, la debe asumir la Direc-

ción General o delegarse directamente a la Unidad de Informática. Ya - sea una u otra, deberán establecer objetivos que se alcancen mediante - el sistema de seguridad y que pueden ser los siguientes:

- Proteger y conservar los activos de la institución contra_ los riesgos de fuego, inundaciones, sabotaje, revelación de información, vandalismo, etc.

- Preservar la capacidad de la institución para subsistir a_ tales riesgos y asegurar su funcionamiento posterior, en - caso de que sucedan.

- Asegurar la integridad y exactitud de los datos requeridos para una efectiva planeación y dirección de la institución.

Para que se puedan alcanzar tales objetivos, es necesario que se_ cumplan las disposiciones del sistema de seguridad. Para realizar ésto se necesita que la Dirección General o la Unidad de Informática, quien_ sea responsable, esté bien enterada de todos los aspectos del diseño -- del sistema de seguridad y que se nombre al personal que se haga respon sable de cada una de las partes del diseño.

La responsabilidad que tenga la Unidad de Informática será tan -- sólo una parte, del total de responsabilidad de seguridad.

Los analistas de sistemas pueden ser los responsables de las partes del diseño que afectan al hardware del equipo y sus programas, aspectos tales como la identificación de los usuarios y las terminales, el uso de criptografía, alarmas y cerraduras programadas, controles en períodos de falla, reconstrucción de archivos, etc.

Otra persona sería responsable de establecer los controles y procedimientos de operación que se usen en el cuarto de cómputo, el control de calidad de la información procesada, las políticas que regirán en la cintoteca, discoteca, programoteca, los controles que protegerán los datos durante el período de conversión, etc.

Para la seguridad física será necesario dar la responsabilidad a un especialista en esta área, deberá establecer precauciones contra fuego, robo, sabotaje; instalar cerraduras, alarmas, cámaras de vigilancia, etc.

También se deben establecer controles administrativos que regulen la clasificación de la información, su administración, la determinación de qué debe ser clasificado y los procedimientos de respaldo de los Departamentos usuarios en caso de una pérdida catastrófica en el sistema, la persona responsable de estos sistemas puede ser ajena a la Unidad de Informática.

Los auditores internos deben revisar cada uno de los aspectos del diseño del sistema que se refiere a la precisión y seguridad. Se deben asegurar de que el sistema se pueda auditar totalmente y se deben desarrolar guías o técnicas que ayuden a auditorías presentes y futuras.

Para mantener una seguridad estrecha en cualquier edificio y organización, es necesario el servicio de guardias. Esto también es válido en los centros de cómputo, máxime si se desea que sean altamente confiables, por ésto, se debe requerir este servicio, ya sea en el centro de cómputo mismo, o en las localidades donde existen terminales.

2.1 Control de los Programas y Programadores

Todo el sistema que no cuente con las medidas de control indispensables, corre el riesgo de ser dañado por sus programadores. Los controles que se impongan a éstos no significa pérdida de eficiencia, por lo contrario, ésta puede ser el resultado de malos procedimientos para controlar a los programadores.

Es probable que la implantación de procedimientos para lograr este fin, no sean bien recibidos por aquellos programadores que trabajan en forma desordenada, acostumbrados a modificar programas sin documentarlos, a diseñar sus propias pruebas para probar un programa, etc.

En todas las medidas que se adopten, se debe tener en mente la mejora de la eficiencia y de la seguridad para proteger el sistema.

2.1.1 Medidas de Control

Existen ciertas medidas de control, que una vez implantadas, puede proporcionar muchos beneficios. Como ejemplo tenemos las siguientes:

- Dividir las responsabilidades. La división que se haga permitirá evitar que una sola persona pueda cometer un fraude sin ser detectado. El trabajo de programación y el de operación, se debe dividir para ejecutarse por personas distintas, así se evitaría que un programador modifique el procesamiento de ciertas transacciones o que viole un archivo vital en beneficio propio.

- Utilizar sólo programas autorizados. En aplicaciones específicas, por ejemplo una nómina, se deben correr sólo los programas autorizados para esa aplicación. Dichos programas debieron haber sido aprobados, completamente documentados y que residan en la biblioteca de programas.

- Evitar que los programadores manejen el equipo de cómputo cuando se estén utilizando datos vitales. Hacer saber a los programadores que su trabajo es controlado completamente, de tal manera que es posible determinar responsabilidades en el caso de que ocurra un fraude.

2.1.2 Servicios a los Programadores

La división de responsabilidades que se haga en el grupo de programación, necesaria para propósitos de seguridad, se puede cumplir proporcionando servicio a los programadores. La división de labores puede incrementar la productividad de un programador y al mismo tiempo, ser parte del diseño para la seguridad.

En tiempos anteriores, los mismos programadores operaban el equipo de cómputo, pero los procedimientos de operación llegaron a ser tan complejos que se hizo necesario el servicio de operadores especializados.

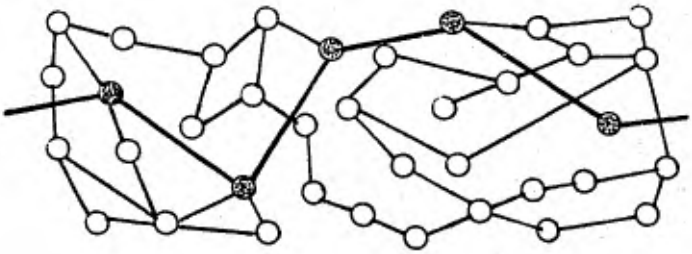
Actualmente, los programadores únicamente presentan sus programas para su compilación sin que se les permita el paso al cuarto de máquinas.

Esto proporcionó un servicio al programador que mejoró su eficiencia, productividad y seguridad.

Se les puede proporcionar otra serie de servicios a los programadores, en su intento por ahorrarles trabajo y mejorar la seguridad. Por ejemplo: un paquete de subrutinas, un macrolenguaje, rutinas microprogramadas, etc.

En varios sistemas existirán una serie compleja de relaciones entre todos los programadores, como se podrá interpretar en la figura No. 1:

F i g u r a No. 1

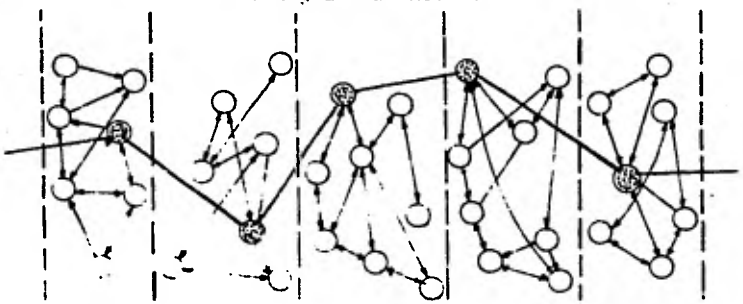


Los círculos pueden representar programas de un sistema. Los - - círculos oscuros y las líneas de conexión más gruesas se pueden interpretar como la serie de programas que procesan transacciones vitales. Esto podría significar una ventaja en el caso de que un programador intente - cometer un fraude, pues necesitaría modificar varios programas para po-- der compensar las desviaciones.

La interpretación varía de un sistema a otro. Algunos círculos - pueden representar programas de aplicación o programas supervisores o - subrutinas, etc. Pero una estructura del tipo de la figura, representa un problema para la ejecución y mantenimiento del programa. El trabajo de un programador afectará el trabajo de otros, puesto que si hace un -- cambio, éste debe ser comunicado a los demás programadores a quienes -- les afecte, para que actúen con conocimiento de las modificaciones.

Una solución a este problema sería dividir el programa de módulos como lo muestra la siguiente figura:

F i g u r a No. 2



La función de cada una de esas fases, deberá estar claramente definida y también la manera como afecta a los demás módulos. De esta manera, cada módulo se puede diseñar u construir en forma independiente - al resto de los módulos. Las interacciones serían fáciles de controlar igual que las modificaciones y cuando éstas afectan las interfases, se_ deberán documentar claramente o cumunicarse a los programadores que necesiten conocerlas. De esta manera, los programadores tendrán un número relativamente pequeño de cambios que conservar y comunicar en lugar_ del diluvio de cambios que darían como resultado de una estructura amorfa.

Una estructura de este tipo mejoraría ampliamente la seguridad, - puesto que para cometer un fraude, se necesitaría modificar varios programas en cada uno de los módulos y ésto sería muy difícil, si se mantiene un control estrecho sobre el trabajo interno de cada uno de los - módulos.

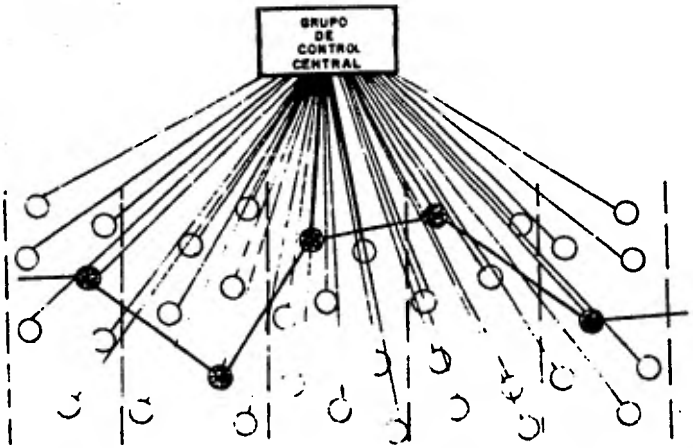
Sin complicidad, un programador sólo tendría conocimiento de las_ interfases entre los módulos.

El programa de control de terminal, la edición de entradas, las - rutinas de pruebas de exactitud, los procedimientos de autorización, -- las rutinas de registro de bitácoras, el proceso de las mismas, los - - programas de los auditores, las rutinas para verificación de etiquetas_ de volúmenes, las rutinas de direccionamiento de archivos, etc., esta--

rán distribuidas en los módulos, sin que los programadores tengan conocimiento de su ubicación.

Otra forma de controlar la programación con una estructura como - en las figuras 1 y 2, sería utilizar un grupo de control, como se ilustra en la figura 3:

F i g u r a No. 3



Este grupo tendrá como función principal, un control y conocimiento total de los programas de los sistemas, así como de los cambios y nuevos programas que surjan. Se encargará de revisar todos los programas y las especificaciones de datos antes de que se graben, para poder tener un conocimiento completo de los que se integran en cada sistema. Asimismo, se encargaría de revisar todas las solicitudes de cambios a los programas y de comunicar tales cambios a las personas que lo necesiten.

De acuerdo a sus funciones, el grupo de control ayudaría a mejorar el sistema de seguridad, puesto que revisaría el trabajo de los programadores desde las especificaciones iniciales de todo programa, así como sus modificaciones y cambios. De esta manera, se podría detectar cualquier intento de fraude de los programadores.

2.1.3 Pruebas de los Programadores

Otra forma de mejorar la seguridad en la programación, es un control bien planeado de los procedimientos de pruebas a los programas. La clave en este control es la división de responsabilidades. No se debe permitir que los programadores se proporcionen sus propios datos de pruebas para sus programas.

Deberá formarse un grupo especial que sea el encargado de proporcionar los datos específicos para comprobar que un programa está correc-

to y que ejecuta lo que se pretende. Los resultados los revisará el -- mismo grupo.

En sistemas donde es de vital importancia la exactitud, los programas tienen que ser probados completamente, cualquier desviación o - - error, deberá ser corregido de inmediato, puesto que de lo contrario, - puede llegar a representar un gran problema posteriormente.

Las pruebas que se hagan a los programas por personas distintas - a quienes las elaboró, prestan un servicio a los programadores, ahorrándoles tiempo, puesto que éstos no tienen que preocuparse por probar sus propios programas.

Asimismo, mejora el aspecto de seguridad, ya que cualquier intento por modificar las transacciones que se procesan con estos progra--- mas, con idea de fraude, sería detectado de inmediato.

2.2 Biblioteca de Programas

Una vez que los programas han sido probados en su totalidad, es - necesario asegurarse que nadie los modifique posteriormente. Para lo - cual se debe catalogar en la biblioteca de programas, en cintas, disco, etc. Si el programa necesita modificaciones posteriores, éstas tam- -- bién deberán ser almacenadas junto con los detalles de quien programó y_ quien autorizó las modificaciones.

De esta manera, proporciona un respaldo en el caso de que llegue a fallar un programa objeto. También se necesita de una estrecha vigilancia para evitar que el volumen que contienen los programas sea leído o modificado por algunas personas no autorizadas.

La biblioteca de programas también le proporcionará un servicio a los programadores, pues les evita el trabajo de mantener en tarjetas o diskettes los programas fuente. En caso de algún cambio, sólo se presentarán algunas tarjetas perforadas o algunos registros en diskette para una nueva compilación.

Se debe tener especial cuidado en que los programas que están catalogados en la biblioteca de programas y que han pasado a través de los procedimientos de inspección y prueba, sean los únicos que se utilicen para el trabajo diario. Cualquier posibilidad de que se pudiera correr un programa no autorizado, para modificar los archivos o la biblioteca de programas sin ser detectado, haría inútiles las demás precauciones tomadas.

2.3 Programas Nuevos

La promoción de programas nuevos para catalogar en la biblioteca de programas, debe seguir un control cuidadosamente planeado.

Será necesario que la aceptación de un programa pase por una serie de autorizaciones de personas distintas y cuyas funciones serán distintas para evitar complicidades.

El programador debe iniciar con una solicitud para promover su programa; en ella debe establecer el propósito del programa nuevo o el cambio que propone. Esta solicitud deberá ser autorizada por:

- El Jefe de Programadores, quien deberá revisar el programa para asegurarse de que pueda ejecutar lo que se pretende.

- El grupo encargado de aplicar las pruebas necesarias para probar el programa, una vez que las pruebas resulten positivas.

- El grupo control de la aplicación que revisa las aplicaciones del programa. Este grupo se encargará de autorizar que sea catalogado en la biblioteca de programas.

  En los sistemas de proceso en línea, el grupo de control encargado de controlar la ejecución del sistema, también deberá dar su aprobación una vez que compruebe que el nuevo programa no degrada en alguna forma la ejecución del sistema.

Los usuarios de las terminales practicarán con el nuevo -- programa para asegurarse que cumple con sus necesidades y que no afecta adversamente en el diálogo hobre-máquina. Además, debe comprobarse que dicho programa no puede ser - modificado desde una terminal. Esta es la aceptación fi-- nal.

En caso positivo, todas las personas anteriores deben firmar una hoja de solicitud del programa, para autorizarlo y para que quede in- - cluido en el archivo de programas operacionales.

La seguridad se incrementa con las diferentes autorizaciones que un programa debe tener; en caso que el programador pretenda crear un -- programa para modificar datos en su beneficio, salvo que exista complicidad entre todos los grupos, sería detectado de inmediato.

Otra parte muy importante en el sistema de seguridad, es el que - se refiere a las operaciones diarias, donde también se deben dividir -- las responsabilidades.

El jefe de la Unidad de Informática debe designar al responsable que estará particularmente interesado en que los procedimientos se lleven a cabo en forma obligatoria y disciplinada. Nombrará a una persona que tendrá la responsabilidad de ver todos los aspectos de la adminis-- tración de la seguridad diaria, deberá trabajar de acuerdo a las indica

ciones que haya establecido el grupo de diseño de seguridad, en caso de observar variaciones en el diseño de los estándares, deberá tomar acciones correctivas. Será la única persona que tenga acceso a las tablas de autorización del sistema e indicará quién puede utilizar determinados programas y cuáles datos.

Tendrá conocimiento de qué usuarios están autorizados para leer o hacer cambios en los archivos; asimismo, tendrá la responsabilidad de la emisión de las palabras clave o de códigos de seguridad, cambios en las tablas de autorización y también asegurarse de que son usadas correctamente. Esta persona examinará los registros de violaciones a procedimientos, revisando la bitácora del operador, las estadísticas de actividades del sistema, los reportes de los guardias, la lista de los trabajos extras y cualquier otro dato que pueda ser índice de infracciones a la seguridad. Estudiando podrá enterarse de los métodos para los cuales se viola la seguridad, basado en ésto deberá estudiar, junto con el grupo de seguridad, la manera de mejorar la seguridad del sistema.

En sistemas con terminales conectadas en lugares remotos, es necesario que exista un encargado por cada una de las terminales en cada uno de los lugares. Esta persona debe de vigilar el buen uso de la terminal, que el personal no viole los procedimientos establecidos, que no descuide sus claves anotándolas en cualquier lugar, etc.

3. Establecimiento del Presupuesto de Seguridad y Precisión en los Controles

Una vez acordado el nivel de seguridad, es necesario establecer un presupuesto para los controles de precisión y seguridad.

El primer paso en el establecimiento de este presupuesto, es determinar hasta qué punto existe el peligro de que la información sea dañada o revelada, o sea, contra qué o quién se están protegiendo los datos, cuál es su valor y cuánto le costaría a la institución si se pierden, se dañan o son revelados.

El establecimiento de controles de seguridad y precisión incrementa el costo de un sistema de computación. Es lógico pensar que a mayor seguridad deseada, más alto es el costo para establecerla, aunque algunas medidas efectivas como lo es una cerradura en una puerta, se puede

lograr con un costo bajo.

El grado de protección así como su costo, dependerá del valor que para un posible intruso, pueden tener los datos de la institución.

Es indispensable jerarquizar la información para determinar si alguien puede obtenerfraudulentamente un beneficio económico al efectuar una modificación no autorizada a ciertos datos, si tal modificación es susceptible de hacerse, si se deben tomar medidas para prevenir tales modificaciones y además si es posible detectarlas en caso de que ocurran. Por ésto, es preciso que las personas que tengan la responsabilidad de la seguridad, junto con los auditores, pongan especial atención a todos estos datos que se refieran a dinero y en general a todos aquellos que se puedan usar para defraudar.

Al hacer el diseño del sistema se debe establecer el costo que implicará para la institución proteger la información contra revelaciones no autorizadas, modificaciones no autorizadas y destrucción.

Puede ser que la información tenga un carácter tan subjetivo que sea difícil ponerle un precio para poder establecer tal costo.

También es necesario jerarquizar los daños que puedan sufrir los diferentes archivos, como puede ser la pérdida completa de un archivo, pérdida de registros simples, modificación de registros y lectura o copia no autorizada.

Es difícil establecer un valor monetario para los archivos de datos, no obstante, ésto serviría para poder situarlos respecto al grado de seguridad que necesitan.

Una vez examinados los valores de los archivos, se pueden establecer los detalles del presupuesto para controles de seguridad y precisión.

4. Controles Necesarios para la Exactitud de la Información

Los controles de exactitud tienen como propósitos principales, -- el de verificar la información capturada para asegurarse que es correcta y completa, asegurarse que los datos de entrada no se procesan dos - veces o que un archivo no se actualice por duplicado.

De manera complementaria, se busca la prevención de fraudes y - - malversación que pudieran cometer tanto los empleados que manejan la información, como personas ajenas al centro de cómputo o inclusive los -- mismos programadores que hayan producido el sistema.

4.1 Verificación.

Una de las pruebas de control más comunes es la verificación de los datos perforados en tarjeta o capturados en disco. La persona que efectúa la verificación en ambos casos, debe teclear los mismos datos que el perforista o el capturista y es la propia unidad verificadora la que compara lo perforado o grabado contra lo tecleado,si algún carácter no concuerda, la máquina se detendrá automáticamente para que el operador haga la corrección que proceda.

4.2 Validación.

Existe también la entrada de datos en línea, en cuyo caso la verificación como tal ha sido substituida por la validación.

En la entrada de datos en línea, los usuarios teclean los datos en los dispositivos con pantalla, mismos datos que van siendo válidos por un programa y son grabados directamente en cinta, disco u otro medio. Debido a que los datos son validados al tiempo de registrarse, cualquier error le es notificado de inmediato al usuario que esté tecleando para que él lo corriga en ese momento.

Esta prueba al igual que la verificación, se puede llevar a cabo en acción separada o efectuarse en línea.

4.2.1 Tipos de Validación.

La validación que se puede aplicar a un carácter puede ser atendiendo a su formato o a sus características particulares.

Desde este punto de vista, los caracteres pueden ser:

Numéricos.- Algunos caracteres siempre deben ser numéricos y además llevar cierto signo.

Alfabéticos.- Algunos caracteres siempre deben ser alfabéticos. Si estos caracteres no son vitales para un procesamiento en lote, dicho procesamiento puede continuar y corregirse después.

Especiales.- Algunos caracteres pueden ser de una serie limitada, que indicarían la clase de alguna transacción.

Signo.- Un carácter indicaría si algún campo numérico es positivo o negativo.

Tomando en cuenta sus características particulares y transaccionales, a los campos también se les puede aplicar dos de las anteriores pruebas, así como las siguientes:

Límite.- Un campo no debe estar arriba o abajo de un límite establecido de antemano. Un sueldo, un recibo de luz, etc.

Rango.- Esta se aplica a un campo numérico para asegurarse que está dentro de cierto límite inferior o superior.

Razonabilidad.- Esta se puede aplicar a un campo numérico para probar una situación normal, puede ser una amplia prueba de rango. Por ejemplo: el importe de un recibo de luz no debe ser igual para un particular que para una empresa.

Validez.- Esta se puede aplicar a un campo que represente un número de partes, un código, un número de empleado o el de una orden de trabajo. Esta prueba tiene el propósito de asegurarse que se afecten los registros debidos, al tratar de actualizar o de accesar un archivo.

Consistencia.- Dos o más campos pueden ser probados en forma relacionada para asegurarse que siguen ciertas reglas de consistencia. Por ejemplo: en una reservación para un vuelo a Guadalajara, la prueba se haría para comprobar que el número de vuelo realmente es el que va a Guadalajara.

Secuencia.- Algunas veces algunos campos deben estar en alguna secuencia predeterminada que servirá para un proceso adicional.

Especiales.- Algunos campos pueden tener pruebas únicas a ellos_ como puede ser la fecha, en la que se revisará que el mes está entre -- uno y doce, el día entre 1 y 28, 29, 30 ó 31, dependiendo del mes.

Una prueba muy importante es usar dígitos verificadores, los cua_ les son derivados de algún algoritmo. Este proceso se aplica general-- mente a campos numéricos, puede ser un número de orden, número de un em_ pleado, etc., a los cuales se les agrega un número extra derivado arit- méticamente de los otros dígitos. En caso de error en el número de or- den o de empleado, el dígito verificador no sería el mismo que el deri- vado de los otros dígitos y ésto causará un mensaje de error, ya sea -- por pantalla o en forma impresa en un listado de validación. Habrá oca_ siones en que se escapen pruebas cuando se intercambien accidentalmente dos o más dígitos en forma compensada, ésto dependerá del proceso de de_ ducción del dígito verificador que se haya escogido.

Es necesario también, hacer pruebas a transacciones para verifi-- car la interrelación de dos o más campos. Algunas de estas pruebas pue_ den ser las siguientes:

Integridad.- Esta prueba sería para comprobar que no se están -- perdiendo campos obligatorios.

Consistencia Interna.- La transacción puede contener campos que_

se prueban unos con otros, como puede ser el número y nombre de un - -- cliente.

Consistencia Externa.- Los datos dentro de una transacción pue-- den ser comparados en una prueba diferida con otros datos en los archivos para asegurar algún tipo de consistencia entre las transacciones.

Secuencia.- Algunas veces ciertos campos dentro de una transac-- ción deben estar conforme a una secuencia establecida, tales como los - tiempos de una serie programada de las operaciones de una máquina.

Números Secuenciales.- Cuando es importante que se controle cada documento, se les puede dar un número secuencial. Esto se hace con los cheques bancarios y con otros documentos.

Validez.- Esta puede ser una prueba más de seguridad que exacti- tud, pues se puede comprobar si determinada transacción está permitida_ para leer o modificar la información que solicita.

Se debe tener presente que las transacciones deben estar diseña-- das de tal forma que se les pueda aplicar estas pruebas.

4.3 Procesos en Lote

Los controles más comunes, y quizá los más importantes, son los que

prueban la integridad y precisión de un lote como un todo. Estas pruebas pueden ser:

Suma de Transacción.- Esta prueba es el número total de tarjetas perforadas en el lote, las tarjetas se van contando cuando se van perforando y al final de la perforación, el número total de tarjetas perforadas se mete en una tarjeta de control del lote, si existe discrepancia indica que una tarjeta se perdió o se procesó dos veces, posiblemente si ocurrió un atascamiento en la lectora de tarjetas.

Totales de Control.- Esta prueba también se hace con la tarjeta de control, se acumulan todos los campos cuantitativos para producir una serie de totales del lote. Estos totales se pueden hacer no sólo con campos cuantitativos donde los totales tienen algún significado, sino también con campos sin sentido, como puede ser la suma total de los números de cuenta.

Número de Lote.- Se pueden revisar los registros para asegurarse que forman parte del lote en cuestión. El número de lote puede estar en todos los registros del mismo.

4.4. Entrada de Datos en Línea

Actualmente en la mayor parte de los centros de cómputo, la infor

mación se alimenta mediante tarjetas o discos. Sin embargo, cada vez - con más frecuencia vemos el uso de terminales en línea para teclear directamente los datos, ya sea en cinta magnética u otros medios. Las -- ventajas de la entrada de datos en línea pueden ser:

- Algunos errores al teclearlos pueden ser detectados y corregidos de inmediato. La operación de verificación utilizada en perforación de tarjetas se evita y se utiliza la - - prueba en línea.

- El proceso de entrada de datos es más rápido. No es necesario suministrar todos los datos, pues el computador puede completar alguno de éstos, cuando son indispensables, - desde sus archivos en línea.

- Por la rapidez de la operación y la detección de errores - en línea, son necesarios menos operadores.

- Las terminales conectadas por teleproceso para la entrada de datos pueden estar localizadas en lugares remotos y diseminados de acuerdo a las necesidades de cada usuario en particular.

Algunas de las desventajas que representa en la entrada de datos en línea pueden ser las siguientes:

- Se requieren programación y mantenimiento de las rutinas - de entradas de datos.

- Los costos del teleproceso o de la unidad central de proce samiento pueden ser muy altos.

- Es necesario equipo de respaldo, ya que de lo contrario -- los usuarios estarán ociosos cuando falle el equipo.

Debe ponderarse la situación particular de cada unidad de informá tica para poder concluir si pesan más las ventajas que las desventajas.

4.5 Pruebas Durante el Proceso.

Este tipo de pruebas son para asegurarse que en los programas se es tán ejecutando correctamente las instrucciones previstas. Como ejemplo de estas pruebas tenemos las siguientes:

4.5.1 Aritméticas.

No es necesario comprobar si una suma, resta, multiplicación o di visión está correcta. La aritmética del computador se puede asumir co- mo infalible, salvo en caso de falla del equipo. Sin embargo, las - -- pruebas aritméticas sirven para asegurarse que no se pierdan cantidades, que los débitos balacean con los créditos, etc.

4.5.2 Redondeo.

Los errores por redondeo pueden representar variaciones significativas al grado de que fueran inclusive objeto de un fraude.

Es necesario preveer esta situación, ya sea mediante el uso de un mayor número de decimales o de alguna forma controlada de compensación.

4.5.3 Cifras de Control Internas.

Esta prueba tiene el propósito principal de hacer una verificación interna de los datos en la entrada.

Consiste en alimentar junto con ellos las correspondientes cifras de control por lote y/o por documento, para que éstas sean compensadas internamente con aquellas que el programa ha obtenido con los mismos campos y conforme a los formatos previamente definidos.

4.5.4 Transacciones Ficticias.

Otra prueba de validación durante el proceso se puede aplicar incluyendo una transacción ficticia, de la cual se conocen los resultados a obtener, en caso contrario, será indicación de que el proceso no está totalmente correcto.

Es preciso que todas las pruebas empleadas no retrasen innecesa-- riamente el proceso, en el caso de que las transacciones sean rechaza-- das o de que fallen algunas de las pruebas de la validación. El proceso no debe detenerse, a menos de que las fallas detectadas hagan inútil la continuación del mismo. Los controles y totales por lote y por documento deben ser diseñados para que cuadren en todos los casos, de manera que pueda detectarse en cualquier momento la pérdida o el rechazo de una transacción.

4.6 Validación de Salidas

4.6.1 Razonabilidad.

Esta prueba al igual que las que se hagan a los cálculos aritméticos ya mencionados, para aplicarse en la entrada o durante el proceso - de los datos, se pueden aplicar a las salidas obtenidas por el computador.

4.6.2 Números Secuenciales.

También ya mencionados son muy necesarios en cheques y documentos financieros para ayudar a una auditoría y en el registro contable de -- los mismos.

4.6.3 Registro de Control.

Al final de toda corrida se debe de grabar una etiqueta de control, que puede contener los siguientes datos: etiqueta identificadora, número de archivo, número de lote, fecha de creación, ciclo de retención, -- número real, una cuenta de registros que están en el carrete, controles_ del lote y cifras de control de todos los campos importantes.

4.7 Controles Externos

Toda información de entrada o de salida, debe pasar antes por una sección de control. Esta puede estar constituida por un empleado en un sistema grande. Este grupo de control es el punto intermedio entre los departamentos usuarios y el departamento de operaciones del computador._ Las responsabilidades de este grupo son las siguientes:

- Recibir para el proceso de trabajo de los departamentos -- usuarios, registrar la recepción del trabajo junto con el_ número de documentos y las cifras de control, notificar al departamento usuario sobre las diferencias que surjan en-- tre éstas y las cifras obtenidas por la propia sección de - control, así como la corrección en casos autorizados, de - las cifras parciales y/o totales.

- Llevar los documentos para su perforación o captación. -- Debe asegurarse que ningún documento se pierda en esta operación.

- Revisará los resultados de la validación de entradas y en_ casos de error, verá que se vuelva a perforar o a incluir_ algún dato. Los resultados de esta validación los compa-- rará contra los enviados por los departamentos usuarios.

- Obtendrá las cintas y discos necesarios de la biblioteca - y los devolverá una vez que se hayan usado.

- Recibirá los trabajos para su procesamiento al Departamento de Operaciones. Esta acción debe estar debidamente documentada a través de una orden de proceso.

- Recibirá las salidas del computador y verificará que las - cifras y los totales de control sean correctos; si no lo - son, investigará las causas, las corregirá y procederá a - ordenar una nueva corrida del trabajo.

- Registrará los detalles de la corrida, posiblemente archivando la última página de la impresión del programa de - - aplicación y la última página del listado en la cual el -- sistema de operación imprime detalles de la misma.

- Enviará los reportes de la salida a los usuarios.

El objetivo principal de la Sección de Control, es establecer - - una función de control de calidad, antes y después del proceso.

Los errores deben ser analizados en función de su origen, tipo, - cantidad, magnitud y cualquier otro factor que ayude a controlarlos. -- Cuando son detectados por pruebas programadas es recomendable mantener_ estadísticas de ellas. Por ejemplo, las paradas del computador, las -- intervenciones del operador o cualquier otra indicación de problemas -- que puedan ser analizadas con el objeto de ejercer presión para minimizar el número de errores.

El control de calidad en la actualización de archivos en línea, - es especialmente importante, ya que al ser afectados éstos desde terminales, existe un gran riesgo de error si no se usan los controles apropiados.

4.8 Procesos en Tiempo Real

En los sistemas de proceso en tiempo real, no es posible utilizar los mismos controles de exactitud que son comunes para el proceso en lote. La razón reside en el hecho de que la mayor parte de la información de entrada es alimentada de manera intermitente, conforme se va -- presentando, y muchas veces aisladamente, por tratarse de procesos y -- hasta sistemas distintos.

En un sistema en el cual el usuario no afecta directamente la información almacenada, es más fácil proteger al sistema de los errores que comunmente se cometen para tal concepto.

El principal problema consiste en ayudarlo a encontrar la información deseada cuando use incorrectamente la terminal.

Pero cuando los usuarios si accesan directamente los archivos, es entonces necesario establecer una serie de controles para evitar errores que puedan dañar o modificar incorrectamente a la información.

Tales controles cobran mayor importancia, debido a que en los sistemas en tiempo real, existen normalmente varios usuarios, diseminados en distintos lugares, lejanos unos de otros, alimentando simultáneamente información al computador.

Esta situación dificulta obviamente su control individual, a diferencia de lo que sería si estuviera en una sola oficina, como sucede en el caso de los perforistas.

Incluso el concepto de mesa de control, en una sección de perforación, no se utiliza por el hecho de que las transacciones son independientes una de otra, y por lo tanto, no se pueden manejar los totales de control que caracteriza a los procesos en lote. Además, debe contemplarse la posibilidad de que se originen errores cuando falle alguna

terminal, la línea de transmisión o el mismo computador principal.

4.8.1 El Diálogo Hombre-Máquina

Existe un factor a favor de los sistemas de proceso en tiempo - - real que es el diálogo hombre-máquina. Si éste está bien diseñado, muchos de los errores que cometa el usuario desde la terminal, podrán ser detectados al momento mismo de la transmisión y rectificarse de inmediato. Para ésto es necesario tomar en cuenta ciertos aspectos que puedan garantizar exactitud en la información procesada y que pueden ser los - siguientes:

- Estructurar debidamente el diálogo hombre-máquina, de tal manera que disminuyan las posibilidades de error del usuario y detecte estos inmediatamente en el caso de que ocurran.

- Planear el sistema para facilitar la correción inmediata - de errores detectados.

- Respaldar la detección de errores con inspecciones de archivos fuera de línea y establecer cifras de control para poder balancear los totales del proceso.

- Establecer los procedimientos necesarios para evitar errores

durante períodos de falla y para la recuperación del sistema en caso de interrupción.

Establecer controles estrechos para prevenir el acceso a archivos o el manejo de terminales por personas no autorizadas.

La importancia que se dé al diálogo hombre-máquina para informar de inmediato al usuario acerca de un error cometido, puede encerrar a su vez un peligro, puesto que el usuario mismo puede desarrollar una actitud de descuido en su trabajo, confiado en que cualquier error que cometa será detectado. Una forma de evitar esta situación, será la de anotar los mensajes de error desplegados y llevar estadísticas de ellos. Esto permitiría encontrar al que comete más errores y contar también, con elementos que permitan ejercer presión sobre los usuarios para que éstos sean más cuidadosos en su trabajo.

4.8.2 Tipos de Validación

El soporte que tiene el proceso en lote representado por el grupo de control encargado de revisar las entradas y salidas de información, no existe en el proceso en tiempo real. En cambio, en este proceso, es posible verificar la exactitud de una transacción simple en forma más completa que en el proceso en lote. Estas pruebas periódicas a grupos de transacciones cuando sea posible; inclusive, se puede detectar poste

riormente un error que se haya cometido en forma desapercibida.

Todas estas pruebas deben estar respaldadas con exámenes de ar- - chivos.

Validación de Transacciones Simples.- Las pruebas que se pueden_ aplicar son numerosas y pueden variar de un sistema a otro. El encarga do de diseñar estas pruebas debe pensar en todas las posibilidades; se leccionar las adecuadas para verificar las entradas tan estrechamente - como sea posible. Una de las pruebas consiste en mostrar al usuario lo_ que ha tecleado, ya que puede haber invertido algunos números y al mostrárselo nuevamente, él puede darse cuenta de su error.

Las pruebas para un carácter o campo de una transacción, ya han - sido explicadas. También es aplicable la prueba de secuencia.

En algunas ocasiones los eventos deben suceder en una secuencia - fija y una desviación de la misma indicará un error.

En un sistema de control de producción por ejemplo, se pueden registrar detalles de los trabajos que se empiezan, que se completan o -- que por alguna razón se cancelan, tomando como referencia el número del trabajador, el número de orden del trabajo y el número de la máquina -- que se utilice. Así, se puede comprobar qué obrero ha estado trabajando bajo cada orden y en cuál máquina.

También se puede detectar una contradicción interna, como por - - ejemplo, en el caso de que se asignara al obrero a otra orden de producción sin darlo de baja en las primeras de ellas.

Otra prueba consiste en validar que todos los datos requeridos hayan sido alimentados. Por ejemplo, si el usuario intenta cortar el diálogo antes que tales datos hayan sido tecleados, el computador preguntará entonces por los datos faltantes.

Validación de grupos de Transacciones.- Resulta de mayor conve-- niencia hacer validaciones por grupos de transacciones que a transacciones simples aisladas.

En sistemas en los cuales se maneja información sobre dinero o valores, será necesario realizar auditorías internas a intervalos regulares para verificar el total del efectivo que debe haber hasta determinado momento.

Para ésto, deberán utilizarse acumuladores que permitan efectuar_ estas auditorías. También se pueden llevar totales de ciertos datos -- que revistan un interés especial, con el objeto de que sean comparados, a intervalos variados o al final del día, contra los acumulados obtenidos por el computador; estos totales son muy valiosos cuando se presentan fallas en el equipo a medio proceso.

Otra forma de validar la exactitud de la información, es el uso - de puntos de referencia.

Estos puntos son establecidos de antemano en diferentes partes de la información y sirven para regresar a ellos y verificar visualmente - si no ha habido omisión alguna.

Aunque este procedimiento puede ser utilizado en forma opcional - por el usuario, resulta más conveniente hacer obligatorio su uso.

Errores detectados posteriormente.- Puede ser que un error no -- sea detectado en el momento en que se comete, sino que llega a ser aparente posteriormente, cuando se verifican los datos previamente almacenados. Es importante que en este caso, quede una constancia escrita -- tanto del error como de la corrección, especialmente si el usuario encargado de hacer ésta, es distinto del que hizo la entrada originalmente.

Detección de errores fuera de línea.- Muchos de los errores cometidos pueden ser resueltos más eficientemente por el mismo usuario que_ haya efectuado la transacción, razón por la cual la retroalimentación - de información que se le dé a éste, será de gran importancia. En algunos casos, esta información no puede ser directa e inmediata, ya sea -- porque el operador esté fuera de línea o porque se está utilizando una_ terminal sin capacidad para dar retroalimentación impresa. En este ca-

so, la solución consiste en instalar una impresora aunque sea pequeña, pero que permita el diálogo mínimo para proceder a la corrección de los errores informados.

4.8.3 Corrección de Errores por Usuarios Especializados

En ocasiones en que una serie de datos provoque una indicación de error, la correción puede ser hecha por un usuario distinto de aquél que hizo la alimentación respectiva. Esta persona debe tener un conocimiento completo de la situación. Puede ser una sola persona o un grupo de ellas.

Estas personas podrán utilizar listados de las corridas de exploración de archivos. Inclusive, puede ser que el manejo de un archivo importante sea asignado a una persona específica, quien sería la responsable de su exactitud y seguridad. Así, al surgir discrepancias dentro de ese archivo, él las investigaría y haría las correcciones pertinentes.

4.8.4 Sección de Control de Entrada y Salida

Esta sección no existe de la misma forma que en los procesos de lote. En los sistemas de tiempo real tendrán funciones distintas y pueden estar situados en los mismos lugares donde se originen las transacciones o estar en otras áreas con su propia terminal. Algunas de sus funciones serán las siguientes:

- Ser notificada, en tiempo real, de cualquier error no re-- suelto en el diálogo hombre-máquina, para investigarlo y - corregirlo.

- Cuando se hagan pruebas a grupos de transacciones, tales - como balances periódicos, la sección de control será notificada de cualquier diferencia resultante para proceder a su investigación y corrección.

- Controlar la actividad de la terminal para investigar alguna acción del operador que rompa las reglas establecidas.

- Puede ser responsable de la precisión y seguridad de los - archivos, incluyéndose las operaciones de exploración y balance de los mismos.

- También puede ser responsable de los controles de seguri-- dad que se utilicen en el sistema. Cualquier violación -- sospechosa a la seguridad, le será notificada en tiempo -- real, además de que se revisarían las bitácoras de seguridad.

Este grupo de control interactuará en la solución de los errores, con diferentes usuarios del sistema. Por lo tanto, es necesario que se establezcan procedimientos en donde se definan las funciones de cada --

uno de ellos y que hagan los diagramas de los procedimientos.

4.9 Controles de Exactitud en Teleproceso

En un sistema de teleproceso, la mayor proporción de errores provienen de los operadores al momento de teclear, más que del proceso - - mismo de la transmisión. No obstante, las faltas de equipo o de terminales, aunque son menos frecuentes, también representan un riesgo importante. En ambos casos, se requieren controles de exactitud apropiados, para asegurarse que la información transmitida sea recibida y procesada íntegramente.

Entre los códigos de control desarrollados en la actualidad, existen algunos que proporcionan un grado de seguridad bastante satisfactoria. Su aplicación dependerá de las condiciones particulares de cada - instalación y del nivel de eficiencia que requiera tanto para detectar errores, como para corregir aquellos que pudieran ocurrir.

Los controles de exactitud, (validación, cifras de control, etc.), relacionados con los errores manuales que cometen los operadores, ya han sido tratados en las secciones anteriores. En la presente sección se - - abordará el tema de los diferentes códigos de control, de que actualmente se dispone, para obtener exactitud en la transmisión de los datos -- por teleproceso.

4.9.1 Criterios para Seleccionar los Códigos de Control

Criterios básicos que deben seguirse al seleccionar los códigos - de control que sean más convenientes para un sistema de teleproceso:

- Analizar la eficiencia de los códigos
- Determinar el impacto que los requerimientos de memoria y - almacenamiento del código pueden tener sobre el rendimiento global del sistema.
- Evaluar el costo-beneficio del código de control

En la mayoría de las instalaciones con teleproceso, predomina el objetivo de lograr el máximo de protección con un nivel razonable de -- los costos respectivos. El impacto sobre el rendimiento de los siste-- mas no afecta mayormente la selección del código de control, ya que - - este problema puede ser resuelto mediante el uso de modems de alta velocidad y/o con la adición de más líneas de comunicación. Por estas razones, ha predominado el uso de códigos de control simples que se caracterizan por un alto grado de redundancia pero que no inflen considerablemente los costos correspondientes.

En el pasado, el alto costo de los circuitos para detectar y co-- rregir errores era determinante en la sección de los códigos de control.

En la actualidad, gracias a los avances tecnológicos en circuitos integrados, el costo de códigos mucho más complejos, es considerablemente - más bajo. Todavía más, los requerimientos de seguridad en la transmi-- sión de datos son actualmente mucho mayores que en los albores del tele proceso. Una de las ventajas de los circuitos altamente integrados, -- que permiten inclusive manejar códigos polinomiales de orden superior, consiste en que no implican un alto grado de redundancia, y por lo consiguiente, no provocan mucha degradación en el rendimiento del siste-- ma.

Como se verá más adelante, los códigos para detectar errores, no requieren una gran proporción de redundancia para poder obtener altos - índices de seguridad. Es posible proteger muy bien un lote de datos -- grande mediante un número de bits relativamente pequeño. Esto se debe a que la potencia para detectar errores depende principalmente del número absoluto de bits verificadores en un grupo de caracteres, más que el porcentaje relativo de los mismos. Obviamente dicha potencia estará -- también determinada por la naturaleza del propio código.

4.9.2 Bits de Paridad

La validación de bits de paridad es la técnica más usada en el teleproceso para controlar la exactitud de la información, debido al bajo costo de su implementación. Sin embargo, su eficiencia es muy relativa

ya que un solo bit de paridad puede no detectar un error, si este último afectara a un número impar de bits; es decir, que el error queda compensado de manera tal que el bit de paridad continuara siendo válido -- aún dentro de la condición misma del error. La causa de este efecto - se debe a que la transmisión de datos en un simple estallido de ruido, o una breve interrupción del flujo de datos, es frecuentemente de mayor duración que el tiempo requerido por un bit, no solamente cuando se - - transmite a altas velocidades, sino también cuando la proporción de - - bits por segundo, es baja. Al respecto, la CCITT[3] hizo un estudio en una línea de telégrafos con cincuenta bauds, donde se obtuvieron los siguientes resultados:

Un estallido de ruido con un error	50 - 60 %
Un estallido de ruido con dos errores	10 - 10 %
Un estallido de ruido con tres errores	3 - 10 %
Un estallido de ruido con cuatro errores	2 - 6 %

Por otra parte, los resultados de otro estudio realizado por la - American Telephone & Telegraph[4], que muestra el índice de errores obser

---

[3] Grupo A de Estudios Especiales de la CCITT (International Telegraph and Telephone Consultative Committee), Contribución 92, Anexo XII, -- página 131, octubre de 1963.

[4] "Error Distribution and Error Control Evaluation" extractos de la Contribución G.T. 43, Núm. 13, publicado en el "CCITT Read Book", Vol. - VII de febrero de 1960, (The International Telecomunication Unión, -- Génova, 1961)

vados en una red pública, indican que cuando se usa una transmisión de 1,200 bits por segundo, hay un 30% de probabilidades de que el bit de paridad falle en detectar errores en los caracteres transmitidos. En general, las pruebas hechas en transmisiones controladas solamente mediante bits de paridad, han mostrado que esta técnica no puede considerarse como un medio satisfactorio para proteger la exactitud de la información transmitida por teleproceso.

Por último, cabe aquí recordar que el bit de paridad puede usarse para validar un caracter o una transacción. En el primer caso, se habla de una validación vertical de paridad, mientras que en el segundo, se referencia como una validación horizontal o longitudinal, también de paridad.

Al respecto, conviene tomar en cuenta que usando conjuntamente ambas validaciones, se puede lograr un nivel de protección mucho mayor que usando aisladamente cualquiera de las dos variantes. Esta característica se analiza a continuación:

4.9.3. El Código Estándar ASCII [5]

El Instituto Norteamericano de Normas (American Standards Institute), que desarrollo el código ASCII, recomienda que se use simultáneamente una validación de bits de paridad, tanto vertical como horizontal. En este caso, el nivel de redundancia requerido es bastante alto, como lo señala la siguiente fórmula, donde la variable X representa el ---

5 American Standar Code for Interchange of Information.

número de caracteres transmitidos y la incógnita Y la proporción de - - bits de redundancia.

$$Y = \frac{X - 8}{7\ X}$$

Con base en esta fórmula, una transacción de 20 caracteres, requerirá una quinta parte adicional de bits, mientras que otra transacción considerablemente grande requerirá aproximadamente de una séptima parte adicional. Como se verá más adelante, esta proporción de bits de redundancia mayor que la de los códigos polinomiales.

En la siguiente tabla, se ilustra una transacción de tres caracteres de datos en código y con validación ASCII.

Posición del bit 1	1	0	1	0
Posición del bit 2	0	0	0	0
Posición del bit 3	0	0	1	1
Posición del bit 4	0	0	0	0
Posición del bit 5	0	1	0	1
Posición del bit 6	0	0	0	0
Posición del bit 7	1	1	1	1
(Validación vertical)	1	1	0	0

Analizando esta tabla, como cualquiera que contenga más de tres - caracteres de datos, se puede observar que las condiciones para que un error pase desapercibido, consisten en que se produzcan simultáneamente dos errores más que compensen el primero, tanto vertical como horizontalmente. Por lo tanto, se puede llegar a la conclusión de que este tipo de validación puede detectar siempre todas aquellas trasacciones - - que tengan uno, tres y cualquier otro número impar de errores, así como aquellas transacciones, que aunque contengan un número par de errores, éstos no se presenten compensadamente. Al respecto, cabe tomar en cuenta que son muy bajas las probabilidades de que suceda tal compensación de errores.

Cuando un sistema de transmisión es propenso a sufrir errores dobles, existe entonces mayor probabilidad de que ocurra una autocompensación de errores. Esto sucede, por ejemplo, en algunos esquemas de modulación donde los bits está representados por un cambio de estado más -- bien que el estado mismo del impulso. Esta situación es conocida como código transición en lugar de código de estado.

Por otra parte, en algunos modems, los datos son codificados en - pares de bits (di-bits) en lugar de bits sencillos. El transportador - entonces puede estar, en determinado momento, en uno de cuatro posibles estados y llevando uno de los cuatro posibles pares de bits. Debido a que un impulso de ruido puede cambiar un par de bits, si dos impulsos - de éstos se suceden antes de terminar la transmisión de un caracter o --

una transacción, se puede producir entonces un error compensado.

Por lo tanto, se puede deducir que la efectividad de una validación de bits de paridad combinados, depende en gran medida del tipo de modulación que se use. Dicha efectividad puede ser más baja cuando se usa el código de transacción en lugar del código de estado, y también cuando se usan di-bits en lugar de bits sencillos.

En general, se puede afirmar que la codificación horizontal y -- vertical de bits de paridad, contribuye considerablemente a disminuir la proporcion de errores no detectados en una transmisión por teleproceso.

4.9.4 Códigos M-Tomados de -N (M-Out-of-N)

Este tipo de códigos consiste en usar un número fijo de bits "N" para transmitir cada carácter, donde "M" de esos bits serán siempre - - unos y la diferencia M-N, será siempre de ceros. Un ejemplo de este - tipo de códigos es el comunmente usado código 4-tomado-de-8, en el -- que los caracteres están representados por 8 bits combinados de tal modo que siempre haya 4 bits unos y 4 bits ceros. Esto da un total de - 70 posibles combinaciones, lo cual ciertamente resulta inferior frente a las 256 combinaciones factibles cuando se usan indiscriminadamente - todos los bits, y a las 128 cuando se usa el bit de paridad. Un sistema similar a este es aplicado ampliamente en los circuitos de radio--

telégrafo, donde se usa un código de 3-tomado- de-7. En general, las - combinaciones posibles de un código M-tomado -de-N están determinadas_ por la siguiente fórmula, donde C. indica el número posible de combina-- ciones tomadas de 2^n unos, N el total de bits usados y M el número de - bits uno especificado.

$$C = \frac{N_i}{M_i\ (N-M)_i}$$

Esta técnica proporciona un amplio margen de seguridad en el caso de que un estallido de ruido provocara el mismo cambio en todos los - - bits, ya que detectaría de inmediato este tipo de error. Este tipo de_ error se presenta frecuentemente cuando se usa modulación de amplitud a base de banda, es causado por los aumentos de voltaje en la línea.

Por otra parte, hay otros casos en los que el código M-tomado-de-N pierde efectividad, y es debido a la naturaleza variable del ruido,_ el cual se caracteriza porque un aumento de voltaje es seguido por una disminución considerable del mismo. No es raro observar en estos ca-- sos, que cuando un cero es cambiado en uno, casi enseguida ocurre un - cambio a la inversa. Del mismo modo, cuando se usa un código de tran- sición a di-bits en lugar de bits simples, hay también probabilidades_ de que ocurra un error compensado.

La compañía IBM hizo una serie de experimentos [6] usando el código de 4-tomado-de-8 en transmisiones a través de una línea de voz de 1,200 bits por segundo. Una vez hecha la comparación entre el mensaje original y el recibido, se determinó el número de errores no detectados y se comparó éste contra los resultados obtenidos en los mensajes transmitidos mediante caracteres protegidos con el código de paridad a través de la misma línea. Se encontró que el porcentaje de los errores no detectados usando solamente el bit de paridad era aproximadamente 1.9 veces mayor que el de los errores detectados en el mensaje con código 4-tomado-de-8. Esta proporción es casi la misma que la observada en la modulación de estado y en la modulación de transmisión respectivamente. Por lo tanto, aunque el código de 4-tomado-de-8 representa una ventaja sobre la validación de paridad, la mejoría no es muy significativa, en vista del volumen de redundancia adicional requerido.

Resumiendo, la transmisión de caracteres en código de 4-tomado-de-8, no resulta muy segura, si no se emplea simultáneamente alguna otra forma de validación longitudinal. En la práctica esta validación longitudinal es usada combinadamente tanto en códigos M-tomados-de-N, con el código de bit de paridad.

---

[6] D.T. Tang y R.T. Chien, "Codig for Error Control", IBM Systems Journal, Vol. 8, Núm. 1, 1969.

4.9.5 Códigos Polinomiales

Después de los códigos M-tomados-de-N, los más comunmente usados, como ejemplo, la representación polinominal mensaje 1010001101, será la siguiente:

$$X^9 + 0 \cdot X^8 + 1 \cdot X^7 + 0 \cdot X^6 + 0 \cdot X^5 + 0 \cdot X^4 + 1 \cdot X^3 + 1 \cdot X^2 + 0 \cdot X + 1 = X^9 + X^7 + X^3 + X^2 + 1$$

En este polinomio resultante ($X^9 + X^7 + X^3 + X^2 + 1$), los términos indicarán entonces las posiciones del polinomio original de orden - X^9, donde el coeficiente es igual a 1; es decir, que en esas posiciones el bit transmitido es un 1.

Como se vé, este es un simple modelo matemático de expresar el mensaje - que debe ser enviado. Dicho método puede ser manipulado a través de -- las leyes del álgebra ordinaria, pero con la condición de que se use -- un la suma binaria, donde no se transporta remanente alguno de un término a otro (este método se conoce como el Módulo 2).

Ejemplo de adición en módulo 2 de aritmética:

$$\begin{array}{l} X^7 + X^6 + X^5 + \quad + X^2 + 1 \\ X^7 + \quad + X^5 + X^4 + X^3 + \quad X^2 \\ \hline X^6 + \quad + X^4 + X^3 \quad + 1 \end{array} \qquad \begin{array}{r} 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1 + \\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0 = \\ \hline 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1 \end{array}$$

Ahora bien, para completar el control de exactitud en la transmisión, se requiere de un segundo elemento llamado "polinomio generador" P(x), el cual deberá ser de un grado arbitrario inferior al grado del primer polinomio M(x), pero mayor que cero. Otra condición para el polinomio P(x), es que su término x^0 (el término de orden más bajo), sea siempre igual a uno .

Por ejemplo: para transmitir el mensaje

$$M(x) = x^9 + x^7 + x^3 + x^2 + 1$$

Se podría usar el siguiente polinomio generador:

$$P(x) = x^5 + x^4 + x^2 + 1$$

El grado r de este polinomio es igual a 5, siendo arbitraria la cantidad de términos que se empleen; obviamente, el número de términos no podrá ser mayor de r + 1.

Una vez definidos los dos polinomios, la rutina de transmisión procederá de la siguiente manera:

1) El mensaje M(x) es multiplicado por x^r, agregando r ceros a la derecha del producto resultante (es decir, en las posiciones de menor orden);

2) El resultado es dividido entonces entre P(x), obteniéndose un cociente de Q(x) y un residuo R(x), como se indica a continuación:

$$\frac{x^r \cdot M(x)}{P(x)} = Q(x) + \frac{R(x)}{P(x)}$$

3) El residuo es entonces sumado binariamente al mensaje M(x), alineando el primero con las posiciones de menor orden del segundo.

De esta manera, se obtiene el mensaje transmitido T(x), el cual se puede representar con la siguiente ecuación:

$$T(x) = x^r M(x) + R(x)$$

Para ilustrar el procedimiento descrito, se utilizará el ejemplo que contiene lo siguientes datos

$M(x) = x^9 + x^7 + x^3 + x^2 + 1$

$P(x) = x^5 + x^4 + x^2 + 1$, donde $r = 5$

Lote de datos = 1 0 1 0 0 0 1 1 0 1

1) $x^r M(x) = x^5 (x^9 + x^7 + x^3 + x^2 + 1)$

$= x^{14} + x^{12} + x^8 + x^7 + x^5$

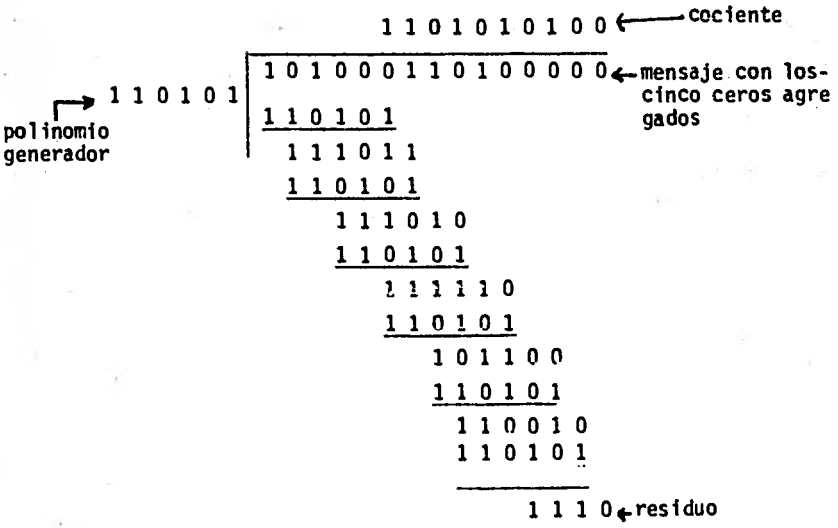
Este último polinomio es equivalente a:

1 0 1 0 0 0 1 1 0 1

Agregando entonces cinco ceros (ya que r = 5), se obtiene lo siguiente:

1 0 1 0 0 0 1 1 0 1 0 0 0 0 0

2) Este resultado se divide entre $P(x) = x^5 + x^4 + x^2 + 1$, obteniéndose el cociente $Q(x) = x^9 + x^8 + x^6 + x^5 + x^2$ y el residuo $R(x) = x^3 + x^2 + x$, el cual es equivalente a 0 1 1 1 0. A continuación se ilustra dicha división



3) El residuo es sumado al polinomio $x^r M(x)$, que se obtuvo como resultado en el paso 1,

$$\begin{array}{ll} & 1\,0\,1\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0 \\ + & \underline{\qquad\qquad\qquad\qquad 0\,1\,1\,1\,0} \\ = & 1\,0\,1\,0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0 \end{array}$$

Este último resultado será entonces el mensaje a transmitir, y estará compuesto como se ilustra a continuación:

$$\underline{1\,0\,1\,0\,0\,0\,1\,1\,0\,1}\;\underline{0\,1\,1\,1\,0}$$

bits originales — bits verificadores

El mensaje es transmitido de izquierda a derecha, por lo que los bits verificadores son enviados al final.

4.9.5.1 Propiedades del Algoritmo a Validar. La división anterior se representa entonces por la siguiente ecuación:

$$\frac{x^r \cdot M(x)}{P(x)} = Q(x) + \frac{R(x)}{P(x)}$$

Por lo tanto,

$$x^r \cdot M(x) = Q(x) + P(x) + R(x)$$

Restando R(x) en ambos términos (la resta y la suma operan de la misma manera en aritmética de Módulo 2), se obtiene la siguiente expresión:

$$x^r \cdot M(x) + R(x) = Q(x) \cdot P(x)$$

Esta ecuación representa entonces el mensaje transmitido, al cual se le identifica convencionalmente como el polinomio T(x).

Por lo tanto, el mensaje transmitido es entonces exactamente divisible por el polinomio generador P(x). Esta circunstancia es precisamente la propiedad del algoritmo que debe ser comprobada en cada mensaje transmitido para encontrar la posible presencia de un error. El computador receptor dividirá entonces el mensaje polinomial entre P(x); si el residuo es diferente a cero, ello indicará la presencia de un error, en caso contrario, no habrá tal, o bien podrá haber ocurrido un error compensado.

Por último, considerando que el error puede a su vez ser representado por el polinomio E(x), un mensaje que se reciba con error será igual entonces a T(x) + E(x).

4.9.6 Patrones de Error y Probabilidades para Detectarlos Mediante los Códigos Polinomiales

La determinación del polinomio generador depende básicamente del

patrón de error que sea común a cada línea de comunicación específica. Estos patrones o características de error que más probabilidad tienen de ocurrir son los siguientes:

a) Errores en un solo bit del mensaje.- En este caso, el error puede ser representado como $E(x) = x^i$, donde i es menor que el número total n de bits del mensaje.

Si se usa un polinomio generador con más de un término, entonces x^i, no puede ser dividido exactamente, por lo tanto, siempre podrán ser detecados todos los errores de bits sencillos.

b) Errores en dos bits del mensaje.- Los errores de bits doble pueden ser representados por el polinomio $E(x) = x^i + x^j$, donde la suma de i + j es menor que n. Por otra parte, si $i < j$, podemos escribir que $E(x) = x^i (1 + x^{j-i})$. Por lo tanto, para poder detectar un error, ni x^i ni $(1 + x^{j-i})$, deben ser divisibles por el polinomio generador que contenga un término con tres elementos.

c) Errores con un número impar de bits.- Si el mensaje contiene un número impar de bits con error, el polinomio que corresponda no podrá ser divisible por $(x + 1)$.

Lo anterior puede ser probado de la siguiente manera: supongamos que un mensaje está representado por el polinomio E(x), el cual sí es divisible por (x + 1). Sobre esta base, podemos escribir entonces que

$E(x) = (x + 1)\ Q\ (x)$. Substituyendo x por 1 obtenemos:

$$E\ (1) = (1+1)\ Q\ (x)$$

Dado que en aritmética binaria $1 + 1 = 0$, tendríamos entonces que $E(1) = (0)\ Q\ (x) = (0)$ Por tanto, E(x) deberá contener un número par de términos.

Con esta demostración concluimos que si se emplea un polinomio generador P (x) que contenga un factor (x + 1), entonces, cualquier mensaje que tenga un número impar de errores podrá ser detectado.

Para ello, cualquier polinomio de la forma $(x^C + 1)$ contendrá siempre un factor (x + 1), ya que $(x^C + 1) = (x + 1)\ (x^{C-1} + x^{C-2} + \ldots + 1)$. Por lo tanto, cualquier polinomio generador de la forma $(x^C + 1)$ podrá detectar todos los errores que contengan un número impar de bits incorrectos.

d) Estallidos de errores.- En este caso, nos referimos a un grupo de bits incorrectos dentro de un mensaje. Definiendo entonces el tamaño de un estallido b, con el número de bits contenidos en un grupo o mensaje, donde al menos el primero y el último bits son erróneos. De esta manera, si E(x) representa el patrón de error 0000010100110000, el tamaño del estallido b será igual a 7.

Factorizando E(x) tenemos la siguiente expresión:

$$E(x) = x^i \; E_1 (x)$$

Donde i es menor que el número de bits del mensaje.

Así, el patrón de error anterior puede ser expresado como,

$$E(x) = X^{10} + X^8 + X^5 + X^4 \text{ ó bien,}$$
$$= X^4 (x^6 + X^4 + X + 1)$$

Dado que x^i no es divisible por P(x), (ya que x^i es un sólo término), el error pasaría desapercibido solamente que E(x) fuera exactamente divisible por P(x).

Cuando el tamaño del estallido b es menor que el término (r+1) -- del polimonio P(x), el polimonio generador $E_1(x)$ no podrá ser detectado. Por eso, si se usa un polimonio generador de 13 bits, todos los estallidos de 12 bits o menos, pueden ser detectados. Para lograr ésto, se necesitan usar 12 bits de redundancia en el mensaje (este número viene a ser el tamaño máximo del residuo R(x)).

Cuando el número de bits en el estallido es igual al del polinomio generador (r + 1) (13 en el ejemplo), el error pasaría desapercibido sólo si el estallido fuera igual al polinomio generador. Ya que por

definición el primero y el último bits son erróneos, los bits restantes (r - 1) del mensaje recibido deben ser correctos. Si todas las combinaciones de bits tienen la misma probabilidad de presentarse, la probabilidad de un error pase desapercibido, será igual a la probabilidad de que un número (r - 1) de bits en el mensaje sean igual al polinomio generador. Esto es igual a $(1/2)^{(r-1)}$. En el ejemplo anterior donde r = 12, la probabilidad de que un error no sea detectado será de $(1/12)^{11} = 0.00049$, lo cual es un evento muy raro.

Cuando el número de bits en el estallido b es mayor que (r+1), hay una variedad de diferentes patrones de error que pueden ser divisibles exactamente por el polinomio P(x). Si $E_1(x)$ es entonces divisible por P(x), podemos escribir la siguiente expresión:

$$E_1(x) = Q_1(x)\, P(x)$$

Siendo $E_1(x)$ un polinomio de grado (b -1), y P(x) otro de grado r, consecuentemente, el grado del polinomio $Q_1(x)$ será entonces (b - 1) - r.

El número de bits que están representados dentro de $Q_1(x)$ será por lo tanto de (b-1-r) + 1 = b-r. Dado que el primero y el último términos de $E_1(x)$ son siempre 1, el primero y el último elemento de $Q_1(x)$ también serán siempre 1. Por lo tanto, habrá (b-r-2) maneras en que $E_1(x)$ es divisible por P(x).

Ahora bien, habiendo $2^{(b-2)}$ combinaciones posibles de bits y si - todas estas combinaciones son igualmente probables, la probabilidad de_ que un error no sea detectado en estas condiciones será de:

$$\frac{2^{(b-2-r)}}{2^{(b-2)}} = 2^{-r}$$

Siguiendo con el ejemplo anterior, donde r=12, la probabilidad de que el error no sea detectado será igual a $2^{-12}=0.00024$, lo cual, toman_ do en cuenta que se trata de un lote que contiene un estallido de un - tamaño mayor que 13 bits, es considerado también como un evento que muy raramente puede ocurrir.

4.9.6.1 Tabla de Probabilidades

Tomando como base un polonomio en el que uno de sus factores sea_ (x+1), y el otro contenga tres o más términos, se pueden obtener los si_ guientes niveles de protección o detección:

Tipo de Error	Porcentaje de protección o Probabilidad de detección
Errores de un bit:	100%
Errores de dos bits (separados o no)	100%
Número impar de bits con error	100%
Estallidos de errores con menos de (r+1) bits:	100%
Estallidos de errores con (r+1) bits exactamente (*)	$(1-(1/2)^{(r-1)})$ probabilidades de detección.
Estallidos de errores con más de (r+1) bits (*)	$(1-(1/2)^{r})$ probabilidades de detección.

(*) Presupone igual probabilidad para cada patrón de error, aunque en la práctica, algunos patrones de error predominan realmente más que otros. Es por ésto que algunos polinomiales generadores de un predeterminado grado r son mejores que otros.

Del análisis de la tabla anterior, se desprende que los códigos polinomiales proporcionan un alto grado de seguridad en la transmisión de datos por teleproceso. Además, mietras mayor sea el grado r del polimonio, mayor será también el nivel de protección contra estallidos de errores.

Sin embargo, en las líneas de voz típicas donde existe una considerablemente alta proporción de estallidos de error largos (por ejemplo: mayores de 30 bits), algunos errores no son detectados por los códigos polinomiales, o, inclusive, por cualquier otro esquema de códigos que pudiera ser razonablemente implementado. No obstante, como se verá en el subinciso siguiente, puede incrementarse el grado r del polinomio, con el objeto de obtener un incremento en la protección que permita compensar dicha situación.

4.9.6.2 Incremento en la Protección

Supongamos que estamos transmitiendo lotes fijos de 100 caracteres (800 bits), a través de una línea telefónica dada, con una probabilidad de 10^{-3} de que el lote puede ser afectado por un estallido de error mayor que 17 bits (lo cual ya de por sí es una consideración pesimista). Si hacemos r = 16 y usamos 16 bits redundantes como protección, la probabilidad de un estallido de error mayor que 17 bits sea detectado, será entonces de $(1 - (1/2)^{16}) = (1 - 1.5 \times 10^{-5})$. A su vez, la probabilidad de que un error no sea detectado es teóricamente del orden de $10^{-3} \times 10^{-5} = 10^{-8}$.

Ahora bien, si hacemos r= 80, la probabilidad de que un estallido de error mauor de 81 bits sea detectado es de $(1 - (1/2)^{80}) = (1-0.83 \times 10^{-24})$, mientras que la probabilidad de que un error pase desapercibido es de $10^{-3} \times 10^{-24} = 10^{-27}$.

Este es un grado de protección mucho mayor del que se requiere para fines prácticos. Para dar una idea del nivel de protección que se puede alcanzar con este último valor de r, podemos decir que si se hubiera estado transmitiendo información protegida de esta manera, en forma ininterrumpida y desde el inicio de la era cristiana hasta la fecha, desde todas las localidades del mundo donde existe ahora un teléfono, a la máxima velocidad de una línea de voz, es sumamente remoto que se hubiera presentado algún error no detectado en cualquier parte del mundo.

Ahora bien, si solamente agregamos 10 bits de redundancia a un mensaje de 100 caracteres de datos, la eficiencia en la exactitud de la información sería mucho mayor todavía que si usáramos la validación horizontal y vertical con el código ASCII. Naturalmente, es de suponer que el costo del equipo requerido para codificar y decodificar los mensajes sería muy alto. Sin embargo, la integración en gran escala de los circuitos, así como su producción masiva, abaten cada vez más los costos respectivos.

4.9.6.3 Validación Polonomial en Mensajes de Longitud Variable

El método que se emplea para este propósito consiste en codificar dos caracteres de validación en cada mensaje, cada uno de los cuales con un número de bits igual al número de bits de los caracteres de datos transmitidos. Por ejemplo, si la longitud de los mensajes variables pueden ser con caracteres de 6 ó de 8 bits, cuando se transmita un men-

saje con caracteres de 6 bits, se agregarán dos caracteres de valida- - ción con 8 bits cada uno. En el primer caso, se obtendrán 12 bits de - validación y en el segundo 16 bits.

Será necesario entonces desarrollar dos polinomios generadores, - uno de orden 12 y otro de orden 16, para que puedan validar los mensa-- jes recibidos, de acuerdo a su respectiva longitud.

Los polimonios resultates serían los siguientes:

$x^{12} + x^{11} + x^3 + x^2 + x + 1 = (x + 1)\ (x^{11} + x^2 + 1)$ y
$x^{16} + x^{15} + x^2 + 1 = (x+1)\ (x^{15} + x + 1)$

De acuerdo con esta teoría, con dicho método, se podrán detectar_ todos los mensajes con uno o dos errores, todos aquéllos con un número_ impar de errores, todos aquéllos con un solo estallido de error menor - que 16 o que 12 bits (según sea el caso), y muchos de aquellos mensa-- jes que tuvieran estallidos de errores grandes; este método ha demos-- trado en la práctica mejores resultados aún que los esperados desde el_ punto de vista puramente teórico.

4.9.7 Códigos para la Corrección de Errores

Teóricamente un código para corregir errores se compone de un -- conjunto de tablas que contienen el carácter, la palabra o el lote co--

rrectos contra los cuales serán compensados los correspondientes bits - tramsmitidos. Para construir este tipo de tablas, se requiere un conoci miento previo acerca de los tipos de errores más probables. Sin embargo, en la práctica, es posible implementar tablas bajo condiciones más - simples.

Cualquiera que sea la forma en que se implemente un código corrector de errores, existe siempre la posibilidad de que se haga una corrección equivocada. En algunas ocasiones, el código cambia un bit correcto en un incorrecto, debido a que el patrón de error particular que ocu- -- rriera en un momento dado, no fuera el indicado para ser corregido por - el código. Si los bits con error fueran distribuidos en random, este -- problema será muy relativo y sucedería muy raramente.

Durante los momentos en que el ruido es excesivo, se incrementa-- ría el número de transacciones rechazadas, provocando con ello una baja considerable en el rendimiento hasta que cesara la distorción. Por otra parte, un sistema de corrección de errores hacia adelante, aunque no degradara el rendimiento, incrementaría el número de transacciones erró- - neas no detectadas.

Comparativamente el sistema de corrección de errores hacia adelan te, implica un costo mayor que el del código para detectar errores por - una parte, mientras que por otra, el número de bits redundantes requeridos, para el mismo grado de protección, es mucho mayor en el primero que en el segundo.

Los códigos para la verificación de errores son muy convenientes para proteger archivos grabados en cinta magnética, disco u otro medio donde al detectar un error, los registros originales ya no estén disponibles. No obstante ello, mediante la transmisión de datos, los registros originales permanencen aún en la transmisora y pueden ser fácilmente enviados una vez más.

Con las técnicas modernas de transmisión mediante líneas duplex completas (full-duplex), de grado inferior e igual al de la voz (voice-grade y subvoice-grade), de banda ancha, los sistemas de corrección de errores hacia adelante, tendría menos mérito frente a los tres criterios para seleccionar los códigos de control. Sin embargo, este código corrector juega un papel importante en algunos sistemas, donde las técnicas de modulación que alcanzan altas velocidades producen una proporción de errores de transmisión mayor que las técnicas usadas en modems de baja velocidad, el porcentaje de errores viene a ser tan grande, que una parte considerable del tiempo de transmisión debe ser usado para retransmitir la información errónea. Es aquí donde se aplica la corrección de errores hacia adelante en el modem para superar tal problema.

Como ya se mencionó, la corrección de errores hacia adelante no corrige todos ellos. Por lo tanto, para lograr una transmisión libre de errores, es necesario respaldar el sistema de seguridad con códigos para detectar errores y con retransmisión en bloques. El papel de la corrección de errores hacia adelante, consiste en disminuir el monto de

retransmisión requerido y, por consiguiente, superar la totalidad del - rendimiento, en las transmisiones que usan una línea de voz a 9,600 - - bits por segundo, este sistema es muy necesario.

4.10 Procedimientos en Caso de Falla del Equipo.

El computador y sus accesorios, al igual que otros aparatos electromecánicos, son susceptibles de sufrir fallas ocasionalmente. Por esta razón, es necesario analizar todos los posibles tipos de fallas, y - determinar lo que debe hacerse cuando cualquiera de ellos se presente. Al respecto, se deben definir mecanismos para asegurarse de que ningún_ dato relevante se pierda o se alimente accidentalmente de manera duplicada. Al mismo tiempo, deberán diseñarse procedimientos para reconstruir archivos en caso de que éstos sufran algún daño de consideración.

4.10.1 Proceso en Lote

En caso de procesos en lote, las fallas del equipo presentan pocas dificultades, debido a que los archivos de salida, una vez actualizados, son grabados en un medio independiente. La corrida en la que -- ocurra una falla, puede ser reprocesada tantas veces como sea necesario. Si se trata de un proceso largo, es conveniente no tener que reiniciarlo desde el principio, por lo cual es recomendable dividirlo en segmentos.

Al final de cada segmento, se puede entonces establecer un punto de control, que sirva como indicador de que se cuenta con las condiciones necesarias para que el proceso pueda ser reiniciado en ese punto. - Estas condiciones pueden ser por ejemplo, que se haya registrado información suficiente, o bien se haya concluido el proceso parcial.

En este punto de control, se haría un corte intermedio de todos_ los acumulados que se usen para el proceso completo. Estas cifras servirán para retroalimentar a los acumuladores, en caso de que el proceso sufriera alguna interrupción y tuviera que reiniciarse a partir del siguiente paso después de cada corte.

Como se verá más adelante, los puntos de control son usados también en teleproceso, cuando se transmiten grandes volúmenes de información. Sin embargo, las características del proceso en tiempo real, implican una situación más compleja para este tipo de controles.

4.10.2 Procesos en Tiempo Real y Teleproceso

A diferencia de los procesos en lote, las fallas del equipo pueden ocasionar grandes problemas en el caso de tiempo real y teleproceso. En la presente sección, se analizan las diferentes medidas de seguridad que se pueden adoptar, en este tiempo de procesos, para prevenir los -- efectos de esas fallas y para establecer los procedimientos a seguir en caso de que se presenten.

4.10.2.1 Mensajes de Recepción

Cada transacción transmitida por una terminal debe generar un -- mensaje, a mera de acuse de recibo, que sea enviado por la unidad receptora. El mensaje puede ser tan rudimentario como un simple señalamiento de asteriscos, pero debidamente programado para señalar que la transmisión ha sido recibida correctamente.

Los mensajes que se usan para señalar que una transacción ha sido recibida correctamente, deberán ser producto de una rutina programada, en lugar de generarse automáticamente como resultado de una función electromecánica del equipo. Esta consideración se fundamenta en el hecho de que los mensajes automáticos del equipo son enviados después de que la transacción ya ha grabado la memoria o en el peor de los casos, después de que un archivo se ha actualizado o se ha grabado en una cinta. Bajo estas condiciones, el usuario no obtendría la señal de recibido, sino hasta que la transacción ya hubiera sido procesada.

Con este procedimiento de mensajes de acuse de recibo, se minimiza el riesgo de que un archivo deje de ser actualizado, si en el instante de la actualización se produjera una falla en el equipo. Sin embargo, subsiste aún la posibilidad de que el usuario de la terminal pueda transmitir dos veces la misma trasacción, provocando con ello una actualización duplicada en los arcnivos. Inclusive, en el caso de una falla brusca en el equipo, no es posible predecir qué tan lejos podrían -

llegar los programas de control para manejar los mensajes comentados, - sería imposible, en un método dado, saber en ese momento, si los archivos fueron o no actualizados.

Por lo tanto, es necesario grabar un indicador dentro de los archivos en el momento que éstos son actualizados, de manera que el pro-- grama de control o el mismo usuario puedan disponer de una referencia - más precisa que le permita saber si la actualización fue o no efectuada.

El indicador requerido puede consistir en un número secuencial - que sea asignado a cada transacción al momento de transmitirla. Este - número puede ser asignado automáticamente por programa, o bien manual-- mente por el usuario. También es posible establecer como indicador algún dato que se obtenga en los registros del propio archivo.

4.10.2.2 Control de Numeración

Este procedimiento consiste en que el operador de la terminal o un programa de servicio, asigne, para cada transacción, un número secuencial de no más de tres dígitos, que sea adicionado como indicador del - registro transmitido. Al ser recibida la información en el computador, cada transacción, entraría en una rutina de programa, donde se verificaría que el número de control asignado fuera una unidad mayor que el último utilizado, se procedería entonces a registrar la transacción enviada.

Una vez que se haya corregido una falla y que la transmisión esté registrada, el operador de la terminal puede retransmitir entonces el último mensaje enviado, para verificar si efectivamente éste fue recibido correctamente. En caso de que así haya sido, la rutina rechazará la transacción y enviará el mensaje correspondiente. De esta manera se evita que la información se registre por duplicado.

Por otro lado, los mensajes que enviará la rutina tendrán también una numeración seriada para cada operador diferente. Este debe checar, a su vez, que los mensajes recibidos conserven su secuencia de control, especialmente después de que una falla sea restaurada. Obviamente, cada operador debe estar plenamente identificado por la rutina, mediante su clave de acceso y/o contraseña (password) correspondiente.

Tomando como punto de partida este concepto básico de control -- por numeración, se pueden desarrollar otras variantes más complejas en función del grado de seguridad que se desee obtener.

4.10.2.3 Bitácoras

La aplicación del concepto de bitácora dentro de la informática, consiste, en su aspecto más simple, en registrar las transacciones de entrada que son recibidas por el computador. Cada una de esas transacciones debe ser grabada en una cinta o en un disco antes de ser procesada, o cuando menos, antes de que sean utilizadas para actualizar un archivo crítico.

El uso de una sola bitácora resulta insuficiente para asegurarse de que ninguna transacción se pieda, ya que el usuario de la terminal no puede saber si la información transmitida, y ya grabada en la bitácora, pudo ser procesada y el archivo correspondiente actualizado. Por lo tanto, es conveniente establecer dos bitácoras; una de transacciones como la que se ha descrito, y otra de actualizaciones, donde se registraría el hecho efectivo de la actualización de un archivo. Después de que ocurriera una falla, los procedimientos de restauración se centrarían en el uso de esas dos bitácoras.

Usualmente, no es necesario registrar toda la información en la bitácora de transacciones, sino solamente aquellos campos que son usados para actualizar un archivo. De manera similar, no es necesario grabar los registros completos de un archivo en la bitácora de actualizaciones.

La utilización de bitácoras no se remite exclusivamente al simple registro de transacciones y actualizaciones. Su uso permite obtener controles más refinados sobre la información de entrada, así como servir de instrumento para el ajuste y/o la recuperación de transacciones.

Entre los principales objetivos de las bitácoras se pueden señalar los siguientes:

- Proporcionar una pista de auditorías que permita seguir la historia de una transacción.

- Facilitar la recuperación de una transacción, para corregir una actualización incorrecta o un proceso, donde desapercibidamente se haya usado un registro actualizado con información errónea.

- Investigar las causas de un registro erróneo.

- Auxiliar en la recuperación de un archivo destruido.

- Auxiliar en la corrección de archivos cuando hayan sido dañados masivamente por alguna falla de programa.

- Corregir o eliminar información falsa que hubiera sido transmitida por el usuario del sistema.

- Detectar violaciones a los procedimientos de seguridad.

La retención de las bitácoras, así como el grado de sofisticación con que se desarrollen, dependerán de las condiciones de la instalación y del nivel de seguridad deseado.

4.10.2.4 Puntos de Control

Este tipo de controles no solamente son usados para procesos en lote, sino también para procesos en línea y en tiempo real. Cuando se envían lotes de información a través de líneas de comunicación, es muy conveniente establecer puntos de control a intervalos fijos y frecuentes del proceso o de la transmisión, de manera que no sean demasiadas transacciones las que deban reprocesarse o retransmitirse en caso de una falla.

Para los sistemas en línea, es preferible conservar bitácoras en lugar de establecer puntos de control. Ello se debe a que, ya se vió anteriormente, las facilidades del sistema de bitácoras permite la recuperación de información entre un vasto número de fallas y errores humanos, inclusive un tiempo después de que el daño haya ocurrido.

Por otra parte, los puntos de control requieren, por lo contrario, menos tiempo de máquina, de controles y de proceso. Este tipo de controles es conveniente en equipos y sistemas donde la rapidez y la eficiencia son factores de primer orden.

4.10.3 Controles Usados en los Diálogos

Todos los controles de exactitud descritos en el punto anterior, son susceptibles de utilizarse en los diálogos hombre-máquina, ya sea de manera aislada o combinados entre sí. También aquí el grado de com-

plejidad que se imprima al diseño de los controles que se adopten, de-- penderá del nivel de seguridad requerido.

En esta sección se hará una exposición suplementaria sobre la importancia de los puntos de control con respecto a las interrupciones y a las revisiones de los diálogos.

El problema fundamental en la interrupción de los diálogos, ya - sea por falla de la máquina, por error humano o simplemente para revi-- sarlo, consiste en la eventual necesidad de repetirlo desde el princi-- pio para asegurar la exactitud del mismo. El problema es aún más grande cuando se trata de diálogos grandes o complicados. Los puntos de -- control son un gran auxilio en estos casos, ya que permiten la continuación de los diálogos a partir de este punto intermedio de los mismos, - así como su revisión y/o corrección parcial sin necesidad de repetirlos completamente.

Los puntos de control deberán estructurarse de tal manera, que - la información transmitida quede almacenada provisionalmente en un dispositivo o computador intermedio, hasta que el usuario de la terminal - teclee la clave para que se ejecute la función deseada. Esta clave tecleada una vez que el usuario tenga la seguridad de que la información enviada es correcta. En caso de que el diálogo se interrumpa por alguna falla del equipo o por un error del operador, éste podrá reiniciarlo a partir del último punto de control establecido.

La frecuencia de los puntos de control dependerá también del volumen de la información a transmitir y de su grado de complejidad o importancia.

Independientemente de que, un diálogo, se necesita volver atrás por motivos de interrupciones o errores, más frecuentemente es necesario hacerlo con el fin de que el operador haga una revisión o vuelva a agarrar el hilo de la información tecleada. Esta segunda necesidad se presenta a menudo, ya que, en muchas ocasiones el operador de la terminal es distraido por una conversación, una orden, una llamada telefónica, o algún otro motivo similar que lo obliga a volver atrás en su diálogo con la máquina.

Asimismo, se puede integrar una rutina que despliegue automáticamente en la pantalla, y a intervalos predeterminados la información tecleada, con objeto de forzar la revisión de ésta, por parte del operador, antes de que se ejecute cualquier función definitiva a través de la terminal.

4.10.4 Control de los Operadores

Uno de los factores de seguridad más importantes para la exactitud en las terminales, consiste en imponer a los operadores de los mismos, una estricta disciplina para el cumplimiento de su trabajo. A su --

vez, esta disciplina deberá estar estrechamente supervisada y controlada mediante programas de validación.

Otro auxiliar importante en caso de falla, es la disponibilidad de manuales que contengan instrucciones detalladas y ampliamente practicadas con anterioridad.

Los controles, entonces, consistirán principalmente en programas de validación procedimientos escritos que precisen claramente las acciones a segurie en caso de falla. Tanto unos como otros, deberán ser el resultado de un análisis minucioso, practicado por analistas competentes y experimentados.

El grado de implementación de los controles en caso de falla, dependerá de las características de los usos a los que se destine la terminal. Cuando ésta es usada sólo para hacer consultas, no existe de hecho el riesgo, ni el problema, de perder información en caso de que la transmisión se interrumpa antes de que termine, bastará entonces con repetir la consulta. En cambio, si la terminal es usada para enviar información cuya exactitud e integridad son vitales, se hace justificable establecer un mecanismo que autosupervise a cada operador.

Junto con el desarrollo de los programas y la elaboración de los procedimientos de control, es indispesanble tomar en consideración la necesidad de contar con planes de entrenamiento y capacitación para los

operadores, tanto de las terminales como del computador. Estos planes incluyen también ejercicios prácticos y simulacros de fallas, con el fin de adiestrar a los operadores bajo las condiciones mismas de la propia realidad. Este aspecto es muy importante, ya que las meras obstrucciones teóricas en el tema en cuestión, no permiten que el operador adquiera conciencia y destreza respecto a sus funciones en caso de falla. Para efectos de tal adiestramiento, es conveniente diseñar programas especiales y los datos de prueba correspondiente.

4.10.5 Medidas de Emergencia

4.10.5.1 Listados Auxiliares

Cuando por cualquier causa el computador falle y las terminales se encuentren fuera de operación, el usuario debe contar con un medio que le permita hacer frente a los requerimientos mínimos de información. Con tal propósito, es conveniente imprimir periódicamente listados que contengan la información básica de los archivos más importantes o más utilizados. Esta información puede, inclusive ser seleccionada conforme a los criterios específicos de cada caso particular.

En caso de que resulte inoperante la impresión de listados para cada usuario, se podría concentrar la información en una oficina central, suficientemente comunicada por la vía telefónica.

En caso de que las terminales estuvieran funcionando fuera de línea, podrían ser utilizadas también como medio de comunicación entre el usuario y la oficina central.

4.10.5.2 Controles Fuera de Línea

Es muy importante que los controles del sistema sean suficientemente efectivos en el momento de una falla, para evitar que se filtre información errónea a los archivos, o que se perdieran transacciones. Es necesario también, disponer de medios de seguridad similares para ser aplicadas en las operaciones que se realicen durante el tiempo que el computador central esté fuera de servicio. Esta consideración es particularmente importante, respecto a sistemas que tengan que ver con el manejo de dinero o de transacciones contables.

Estos controles pueden continuar operando a través de la misma terminal pero fuera de línea. En un sistema que haya sido diseñado con buenas medidas de control, las terminales del mismo deberán contar con sus propios acumuladores. De tal suerte, cuando se presente una falla en el computador central, el usuario podría desplegar en la pantalla o imprimir si tiene el medio correspondiente, los totales acumulados. Las operaciones podrían continuar fuera de línea, y cuando el sistema completo quedara restaurado, se desplegarían nuevamente los totales, para determinar las diferencias que deberán reportarse y que habrán de actualizar y hacer corresponder, los acumuladores de control en los ar-

los archivos del computador. Se imprimiría entonces, el contenido de - estos acumuladores para verificar que hayan sido correctamente actualizados y que concuerden con los de la terminal.

La continuidad en el uso de cifras de control y otras medidas de seguridad durante el lapso de falla, es muy importante para asegurarse_ de que nada haya sido indebidamente procesado durante ese tiempo.

4.11 Recuperación de Archivos

Hay gran variedad de circunstancias que pueden ocasionar daños a un sistema de computación. Algunas de ellas se refieren a siniestros - tan dramáticos, como por ejemplo, un incendio de grandes proporciones - o un atentado terrorista.

Para prevenir este tipo de contingencias, es necesario elaborar_ un plan de emergrencia que contemple los procedimientos pertinentes para restablecer la operación normal de una Unidad de Informática de la - manera más eficiente y en el menor tiempo posible.

Una de las áreas que deben ser tomadas en consideración en un -- plan de esta índole, es la recuperación de archivos, a cuyas principa-- les técnicas se refiere la presente sección.

4.11.1 Daños en los Archivos

Los daños que puede sufrir un archivo básicamente, son de dos -- clases: la primera es cuando solamente quedan afectados algunos registros cuya corrección es relativamente rápida y simple; la segunda clase se refiere a la eventualidad de que un archivo completo o un segmento - grande resulte total o parcialmente destruido y el daño sea tan extenso que no pueda ser corregido manualmente. Aunque este segundo tipo de daño se presenta muy remotamente, sería un desatino pensar que nunca po-- dría ocurrir.

Por lo tanto, dentro de los planes de emergencia para una Unidad de Informática, deben de incluirse los procedimientos dirigidos a la reconstrucción masiva de archivos.

Entre las principales causas de la destrucción masiva se encuentran las siguientes:

- Error de programa
- Accidentes durante la fase de prueba
- Carga y/o actualización de archivos equivocados
- Errores de operación
- Montaje incorrecto de la cinta
- Cinta o disco defectuoso
- Robo de la cinta o disco

- Destrucción de la cinta o disco
- Sabotaje
- Incendio

4.11.2 Respaldo de Archivos en Lote

La reconstrucción de archivos es más fácil en sistemas de procesos en lote que en los de tiempo real, debido a que normalmente se crea un nuevo archivo, ya sea en otra cinta o en otro disco (Figuras 4 y 5), como resultado del proceso en lote, en lugar de actualizar los registros de uno que residiera permanentemente en disco.

FIGURA Nº 4

UNIDADES DE CINTA

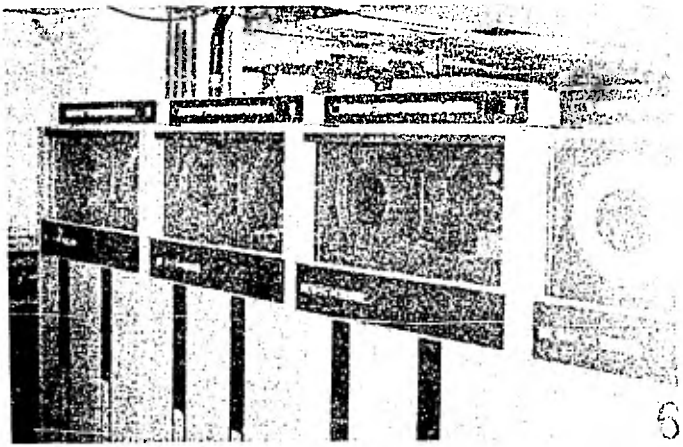
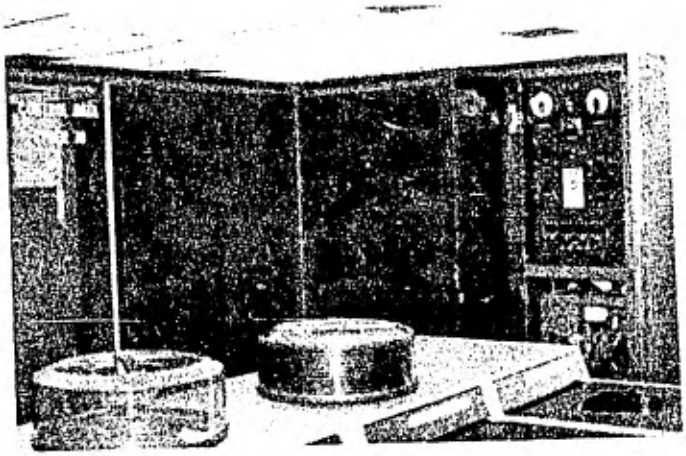


Figura Nº 5

PAQUETE DE DISCOS MAGNETICOS



tualizados. Paralelamente se deben conservar también los archivos con - las transacciones de todos los procesos posteriores a la última copia -- del archivo maestro. De esta manera, se está entonces en la posibilidad de repartir los procesos subsecuentes. El número de archivos que se prevea respaldar de esta manera dependerá de las políticas que al respecto se fijen para cada instalación y/o para cada sistema.

4.11.4 Archivos de Sistemas en Tiempo Real

La reconstrucción de archivos es básicamente similar a la técnica descrita en el punto anterior, consiste en una copia periódica de los -- mismos y en una bitácora que contenga los movimientos efectuados desde - el último copiado. No es necesario registrar todos los mensajes del diálogo entre el usuario y la máquina, sino solamente aquellos cuyo resultado afecte directamente a los archivos. Sin embargo, no deja de resultar más conveniente la conservación de una bitácora de transacciones como la que se comentó anteriormente, ya que tales bitácoras sirven además para lograr una recuperación más completa en caso de que falle el equipo.

Por otra parte, dicha recuperación se puede efectuar automáticamente, sin una nueva intervención del operador, ya que bastaría con reprocesar las transacciones contenidas en la bitácora por medio de un programa especialmente diseñado para tal efecto. Además como se vió anteriormente, por medio de la bitácora se elimina la posibilidad de perder o duplicar una transacción durante el lapso de una falla.

4.11.4.1 Duplicidad de Archivos

En algunos casos es conveniente conservar de manera permanente una copia de los archivos críticos, la cual sería actualizada simultáneamente al actualizar el archivo maestro original. Mediante esta técnica se puede disponer de una copia inmediata, cuando por alguna falla no pueda accesarse el archivo original.

Desafortunadamente, esta duplicación de archivos no escapa a los errores de programa que redundan también en una actualización incorrecta. Por lo tanto, la duplicidad de los archivos no es en manera alguna, un sustituto de las bitácoras de transacciones y/o actualizaciones que se explicaron anteriormente.

Cuando por alguna razón algunos de los archivos quedan fuera de funcionamiento, su restauración posterior se puede hacer siguiendo los procedimientos señalados en el apartado anterior, o bien volviendo a copiar íntegramente el archivo original

4.11.5 Recuperación de Base de Datos

Cuando se tienen archivos de acceso directo pequeños no hay dificultad en copiarlos periódicamente, ya sea en cinta o en disco, y conservarlos con propósitos de recuperación. Por otro lado, se requeriría mucho más tiempo de máquina, para copiar con este mismo propósito, bases de datos que contengan grandes volúmenes de información.

La reconstrucción de tan enormes archivos es una tarea considera-- ble, la cual se ve dificultada por las siguientes circunstancias:

- Los archivos grandes no pueden ser copiados con la misma_ frecuencia que en el caso de los pequeños.

- Aunque la base de datos pudiera ser dividida en regis- -- tros o campos críticos, con el objeto de copiar solamente los primeros sólo cuando sufran una modificación, existe_ el inconveniente de que el ciclo de copiado de los datos_ será siempre diferente, debido a que no todos son actuali zados simultáneamente. Por lo tanto, algunos de los re-- gistros o campos que permanezcan inmutables serán copia-- dos una sola vez, mientras que habrá otros que serían copiados por no recibir ningún movimiento.

  Adicionalmente, los archivos que fueran vitales para las_ operaciones diarias tendrían que ser copiados todos los - días.

En algunos casos, cuando la información sufre escasas modificaciones, resultaría más conveniente obtener el respaldo mediante la actualización de una copia anterior que haciendo una duplicación del archivo. Las bitácoras de transacciones pueden ser utilizadas para este propósito fuera de línea, dentro de lo que sería un procedimiento contínuo que respaldara a los archivos del sistema en tiempo real.

En la actualidad, no existen aún mejores medios para lograr una -- rápida recuperación de grandes bases de datos.

Es necesario por lo tanto, ponderar las ventajas y desventajas de cualquier procedimiento de recuperación en una base de datos, en fun- -- ción de las condiciones propias de cada instalación y del grado de seguridad que se requiera para la protección y la recuperación de bases de - datos.

5. Privacidad de la información

Es importante evaluar el valor que representa la información que se procesa en las Unidades de Informática, para diseñar el grado de protección necesario.

Se debe tomar en cuenta el daño que pueda causar a la institución, así como a terceros, si la información fuera revelada.

Por ejemplo, puede causarse un gran daño a una institución si su información financiera llegase a manos de extraños, de la misma manera que otro tipo de información, penal, médica, etc., podría utilizarse para extorsionar a terceras personas. De ahí que se deben tomar precauciones necesarias para proteger, hasta donde sea posible la información.

5.1 Identificaciones Programdas

Es necesario definir para cada usuario, qué es a lo que tiene -- permiso para realizar consultas, actualización borrar campos o regis- - tros, etc.

5.1.1 Identificación del Usuario

Cuandp se opera un sistema con terminales conectadas, es necesario identificar al usuario que pretende acceder al sistema.

Hay varias formas de identificar a una persona, puede ser por características físicas, ya sean sus huellas digitales, su voz, etc., por algo que la persona sabe o memoriza una palabra clave, las respuestas - a determinadas preguntas, etc., por algo que lleve como una tarjeta, -- una llave, etc.

Características Físicas Personales.-

Existen muchas características físicas para reconocer a una persona com una probabilidad muy baja de error. Algunos dispositivos para identificar pueden ser muy caros como los lectores de huellas digitales, y otros son improbables como pueden ser algunos que pudieran identificar alguna persona por su olor, por la impresión de sus labios, por la configuración de su cabeza, etc.

También es menester considerar si sólo se va a indentificar a la persona o si también se tiene que verificar que él es quien dice que es. La identificación requiere de una investigación más amplia para desarrollar dispositivos que permitan identificar a una persona, la verificación es una simple decisión es una simple decisión binaria (si o no). - Cabe aclarar que cualquier medio de verificación puede cometer dos tipos de errores:

- Un falso rechazo, en el cual la persona original es rechazada

- Una falsa aprobación, en el cual un impostor es aceptado.

Una de las formas para identificar es por medio del reconocimiento de la voz del usuario. La ventaja en el uso de la impresión de la voz para identificar a un usuario es que no necesita un equipo especial la terminal, sino un teléfono. El usuario dice una frase predeterminada y el sonido debe ser convertido en un modelo de bits el cual debe ser comparado con otro modelo previamente almacenado para ese usuario; como normalmente se difiere en tiempo cuando se pronuncia alguna frase se deben establecer límites permisibles de variación. La operación de reconocimiento de voz debe ir asociada con un número de seguridad para que proporcione una medida de seguridad más alta.

Con cualquiera de las técnicas que se utilicen para identificar_ se debe pensar qué métodos pueden utilizar un impostor. Es probable -- que con el reconocimiento de voz una persona aprenda a otra o que grabe su voz y la utilice. La solución en este caso, sería el cambio periódi co de las palabras clave asociadas con el reconocimiento de la voz.

Un problema con el reconocimiento de la voz se presenta cuando - una persona tiene un resfriado. Si los límites de variación permisi-- bles se amplían para aceptar a usuarios con resfriados, entonces se in crementará la probabilidad de aceptaciones falsas.

Otra forma de identificar a una persona se puede hacer midiendo_ el tamaño de los dedos, ya que existe una probabilidad muy baja de que_ dos personas tengan los dedos del mismo tamaño.

Claves Memorizadas.-

Existen otras formas menos caras para proteger la información. - Se le pide al probable usuario que se identifique con una palabra clave u otra información que él sólo debe saber.

Para una medida de seguridad razonable es deseable proporcionar_ a cada usuario un código de seguridad diferente que deberá utilizar jun to con su identificación personal al momento de identificarse cuando -- vaya a utilizar una terminal, después de teclear estos datos el computa

dor verificará que ese código de seguridad ha sido emitido por ese número de identificación.

Es recomendable que los códigos de seguridad se cambien periódicamente e instruir a los usuarios acerca de su custodia para evitar que se divulgen. Asimismo, se deben otorgar las facilidades necesarias a los usuarios para cambiar su código de seguridad cuando lo soliciten, máxime si ellos piensan que alguien conoce su código.

La seguridad de los códigos puede verse comprometida si la terminal los imprime o los despliega en pantalla, por lo cual es importante evitarlo, puesto que una persona ajena puede estar observando y enterarse del código. Se puede prevenir la impresión o desplegado del código para una acción del operador o hacerse en forma automática, lo cual sería preferible. Otro procedimiento sería ocultar el código mezclando su impresión con otros caracteres, este procedimiento puede considerarse más satisfactorio que impedir la impresión.

Es importante que el procedimiento de identificación sea lo más claro y corto posible para evitar confusiones en el usuario, así como proporcionarle un código de seguridad lo sficientemente corto para que lo memorice y evitar que lo anote en una tarjeta que la pueda olvidar en algún lugar.

La desventaja en las palabras clave o códigos es que los puede - obtener otra persona sin que exista una pérdida física o sin que se tengan que duplicar, o sea no existirá evidencia física de que otra persona los posee.

La protección en este caso es utilizar códigos una sola vez, de esta manera, los códigos se vuelven inválidos una vez que se haya utilizado y de nada servirá a un intruso que los haya obtenido casual o deliberadamente.

Para lograr ésto, será necesario proporcionar al usuario una lista de números en lugar de uno sólo, pero se deberá instruir al usuario para que evite marcar los números que han utilizado para que en caso de que los pierda, nadie pueda saber cuál es el próximo número a utilizar. Es probable que después de cada sesión de trabajo el sistema le permita al usuario formar el próximo número que deberá utilizar.

Otra forma de evitar el uso de números o claves repetidos es el de proporcionar al usuario un número o frase de diez caracteres el cual deberá memorizar, así cuando se tenga que identificar, el computador le solicitará ciertos caracteres de su número, por ejemplo el tercero y - el séptimo y cada vez que tenga que identificarse se le solicitará un - par diferente de caracteres

La seguridad en la identificación del usuario, se puede hacer --

más confiable incrementando su complejidad, pero esto encierra el peligro de que llegue a ser tan difícil que el usuario cometa errores y - - arriesgue la seguridad.

Todo uso de códigos de seguridad debe ser rigurosamente controlado para detectar y atrapar a una persona que utilice el código de seguridad de otra persona. Si los usuarios saben que existe una gran probabilidad de que serán atrapados cuando intenten acceder al sistema con - el código de otro usuario, será un factor psicológico para evitar intentos inválidos.

Otra técnica es tener una serie de preguntas y respuestas seleccionadas, donde el usuario sólo conozca las respuestas. Deben ser preguntas que sean imposibles de que se olviden. Este procedimiento tiene la ventaja de ser fácil de utilizar pero la desventaja de ser prolongado en su operación.

Objetos Físicos.- El usuario también puede indentificarse por - medio de algún objeto físico como una llave, una tarjeta, etc., las llaves pueden ser de forma muy complicada y las tarjetas contener identificación codificada óptica o magnética, para identificar al propietario.

Las ventajas de las tarjetas es que no pueden ser duplicadas tan fácilmente como las llaves, pero ambas tienen la desventaja de que pueden ser robadas, ya sea que el usuario olvide la tarjeta o la llave en_

la terminal o que sean sustraídas sin darse cuenta.

El uso de tarjetas magnéticas puede extenderse por ser más práctico que las llaves, sin pretender que su uso mantenderá alejados a los intrusos, pero se pueden hacer más seguras si su uso se combina con códigos de seguridad memorizados, necesitando ambos para poder acceder al sistema.

5.1.2 Identificación del Equipo Receptor

Paralelamente con la identificación de usuarios, es necesario que el computador o el equipo central identifique a su vez a la terminal que intenta comunicarse con ellos. Esto es particularmente importante cuando no todas las terminales interconectadas a través de un mecanismo de distribución por encuesta (polling device), están autorizadas para comunicarse, ya sea total o parcialmente, con el computador o equipo principal. Las causas de una conexión errónea pueden ser de origen, tanto manual al marcar el disco telefónico, como técnico dentro de un aparato interconector de varias terminales, debido a que el ruido de la línea puede cambiar su dirección (Esto último sucede particularmente cuando se usa un sólo bit de partida para detectar errores provocados por el ruido, ya que este tipo de ruidos en la telecomunicación modifica a menudo más de un bit).

Una manera de llevar a cabo dicha identificación, consiste en -- que el computador solicite automáticamente un número de control, tipo - de contraseña que previamente se le haya asignado a cada terminal. La_ respuesta de ésta deberá obviamente ser también automática, y además -- ser un requisito previo antes de iniciar cualquier tipo de acceso.

De esta manera, el computador central procederá a cotejar la contraseña de la terminal contra un archivo de autorizaciones previamente_ grabado y, de acuerdo con el resultado, enviar un mensaje a la terminal para indicarle al usuario si puede continuar la comunicación, o si ésta queda automáticamente cancelada en caso de que se trate de un acceso no autorizado para esa terminal.

En general, este mecanismo actúa de una manera similar a la de - identificación de usuarios, mediante contraseña. Combinando ambos procedimientos, se le da al sistema un grado mayor de seguridad. Sobre todo cuando no todas las terminales están debidamente protegidas, tanto - desde el punto de vista físico como lógico.

5.2 Esquema de Autorización

Una vez que el usuario ha sido identificado por el sistema, el - colputador debe verificar qué tipo de instrucciones están autorizadas - para el mismo usuario. Para tal efecto, es necesario desarrollar un es

quema de autorizaciones, el cual deberá dar como resultado una tabla -- que muestre los diferentes niveles de acceso que estén autorizados para cada usuario. Dichos niveles de acceso se refieren a todo el sistema - en su conjunto. Por ejemplo, consulta, actualización y modificación de archivos, ya sea parcial o totalmente, o bien uso y actualización de -- programas, etc.

Un esquema de autorización consiste en clasificar la información en diferentes niveles o estratos de seguridad por una parte, (clasificación vertical o estratificación), y por otra, en seleccionar a los usuarios o departamentos autorizados para su acceso, (clasificación vertical). Los siguientes cuadros ejemplifican de una manera ilustrativa -- estos dos conceptos:

A) Estratificación o clasificación horizontal:

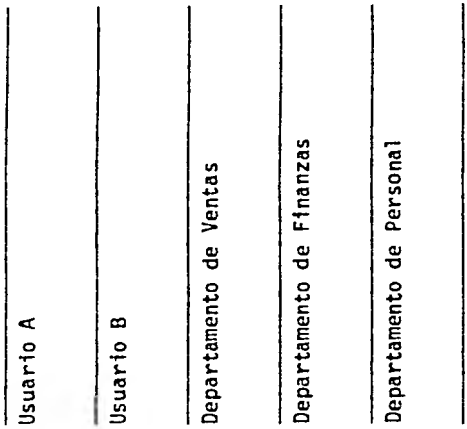
Secreto Máximo

Información Secreta

Confidencial

No Clasificada

B) Clasificación Vertical:



5.2.1 Estratificación

La estratificación o clasificación no sólo debe abarcar a la información accesible a través de la terminal, sino que debe extenderse a todos aquellos medios que de una manera u otra deben ser de uso restringido y controlado (por ejemplo: documentación, cintas y discos magnéticos, equipo periférico e inclusive el manejo de éstos por parte del personal de la Unidad de Informática). Uno de los controles disponibles consiste en etiquetar físicamente las cintas y los discos con una leyenda que señale el nivel de estratificación asignado y el tipo de autorización que debe tener el operador que deba manejarlos. Adicionalmente, se puede instalar una cerradura de seguridad en la unidad del disco (o en el compartimiento de las cintas clasificadas). Igualmente, es conveniente establecer un procedimiento similar para controlar la seguridad de los programas y de los demás recursos de software que estén considerados como clasificados. Por lo que respecta a algunas terminales consideradas inseguras, o impresoras remotas o computadores periféricos, que hayan sido deseñadas con bajo margen de seguridad, pueden quedar inhibidas del acceso a información altamente clasificadas. Las medidas de protección pueden llegar inclusive hasta las mismas hojas de los listados impresos por la computadora, las cuales pueden ser señaladas por programa y mediante la impresora, con una leyenda notoria que indique el nivel de su confindencialidad.

A su vez, las funciones del personal de la Unidad de Informática deberán estar seleccionadas de acuerdo al nivel de autorización asignado a cada persona. Ningún empleado deberá manejar documentos o información que correspondan a un nivel de autorización menor que el suyo. Asimismo, el uso de terminales debe estar restringido a aquellos empleados -- que no cuenten con la autorización correspondiente.

En resumen, la clasificación de información para efectos de su - estratificación en niveles de seguridad, debe abarcar los siguientes aspectos:

a) Archivos y registros de datos
b) Programas
c) Medios de almacenamiento (cintas, discos, etc.)
d) Unidades de cinta y de disco
e) Terminales
f) Cuartos de almacenamiento para material clasificado
g) Listados de la impresora y de la consola
h) Manuales de operación y de soporte
i) Personal de la Unidad de Informática

Desde el punto de vista ideal, el manejo de esta estratificación podría ser controlado automáticamente por el sistema operativo, a manera de una programación integrada u opcional. También podría tomar parte de los programas de aplicación del sistema, (aunque esto último, no garantiza suficiente nivel de protección). Sin embargo, el tipo y ni--

vel de implementación en estas cuestiones, dependerá en última instan-- cia, de las características particulares de cada Unidad de Informática, de la clase de información que ahí se maneje y de los riesgos a que todo ello pueda estar expuesto.

6. Diseño de la Seguridad Física

La seguridad física deberá ser de interés no sólo para las áreas críticas, tales como el cuarto de computadoras, la cintoteca o la programoteca, sino también para cualquier aspecto del desarrollo del sistema.

6.1 Controles Físicos

Los controles técnicos que se discutieron en las secciones anteriores, necesitan ser completados por controles físicos, tales como: puertas aseguradas, bóvedas a prueba de ladrones, precauciones contra incendios, vigilantes y alarmas, tales controles son muy importantes, aunque generalmente no son tomados en cuenta.

Vigilantes.- La efectividad de un vigilante puede realzarse gradualmente si el edificio se encuentra protegido con detectores electrónicos. (Figura Nº 6)

Figura Nº 6

VIGILANTES

Sin éstos, un vigilante no sabría qué es lo que está pasando en los alrededores, así un intruso puede esconderse del vigilante cuando éste esté patrullado.

Deberá existir únicamente una puerta de entrada, en la cual se pueda colocar a una recepcionista que actúe como vigilante durante las horas de trabajo, después de las horas de trabajo, se debe cerrar la Unidad de Informática, la cual debe ser protegida con alarmas contra intrusos y los datos y programas importantes deberán ser guardados en cajas fuertes, bóvedas o almacenes.

Es esencial un botón escondido en el lugar de la recepcionista, para que esté en posibilidad de requerir ayuda cuando sea sorprendida por un intruso.

Para una mayor seguridad, cuando se emplean vigilantes, éstos deben ser contratados de una firma reconocida, como lo es la Policía Bancaria, y no tratar de obtener al más barato disponible.

Se le deben de dar todas las instrucciones detalladas, y debe ser supervisado constantemente para ver que cumpla las instrucciones.

Bóvedas.- Una bóveda es una construcción no removible construida permanentemente en una área permitida. Generalmente tiene una capacidad mayor que una caja fuerte, y si está diseñada apropiadamente pro-

tegerá sus contenidos aun si el edificio fuera destruido completamente_ por un incendio.

Usualmente están construidas de hierro, acero o de fuerte cons-- trucción de concreto, tienen un armazón de hierro y un candado de combi_ nación.

Candados.- Los candados suministran una de las formas más baratas de protección.

Los candados para las puertas críticas deben ser seleccionados - de tal manera que sus llaves no pueden tener duplicados en las cerrajerías, el patrón de la llave no debe estar disponible como una llave comercial en blanco estándar.

Los candados de combinación son generalmente usados en bóvedas y cajas fuertes.

Existen otros tipos de candados operados con tarjetas con codifi_ cación magnética, éstos pueden ser altamente selectivos en cuanto a qué tarjetas pueden aceptar y cuáles rechazar.

Almacenaje Seguro.- Martin James [7], establece cuatro categorías de lugares seguros a prueba de ladrones dentro de un edificio, éstos son:

---

7 James, Martin, Security, Accuracy And Privacy In Computer Systems. New Jersey. Pretince-Hall, Inc. 1980, Pág. 281.

1.- Las cajas fuertes y los contenedores de protección

2.- Las bóvedas

3.- Los cuartos de almacenaje de registros (más grades que una bóveda pero menos seguros)

4.- Las áreas cerradas (en las cuales la gente trabaja)

Las cajas de seguridad y bóveda también pueden hacerse a prueba de incendios para que sus contenidos resistan si el edificio es totalmente destruido por el fuego.

Cajas Fuertes y Gabinetes.- Las cajas fuertes y los gabinetes de registros pueden ser diseñados para proteger su contenido contra el fuego o contra ladrones.

Cuartos de Almacenaje.- Los cuartos de almacenaje de registro son más grandes que una bóveda, pero es menos resistente al fuego y a los ladrones. (Figura Nº 7)

Figura Nº 7

CUARTO DE ALMACENAJE

Si los datos o programas importantes son guardados en el cuarto de almacén, éstos deben ser guardados a su vez en gabinentes a prueba - de fuego y de ladrones.

El cuarto de almacén deberá tener rociadores o algún otro tipo de extinguidor automático.

Areas Cerradas.- Los cuartos donde las personas trabajen, pue-- den ser consideradas como áreas cerradas, deben ser aseguradas para man tener alejados a los intrusos. El cuarto de computadora deberá ser una área cerrada, en la cual como se mencionó anteriormente, puede tener -- sólo una entrada, controlada por un vigilante o una recepcionista o con una cerradura o candado de tarjeta o cerradura en la cual se teclee un código.

Alarmas.- Las cajas fuertes, bóvedas, cuartos de almacenaje de registro de áreas cerradas, deberán estar protegidas con alarmas contra fuego y alarmas contra intrusos.

6.2 Detectores y Aparatos de Seguridad Eléctrica

6.2.1 Tipos de Dispositivos de Detección

Existen muchos tipos de dispositivos de detección, cada uno de - los cuales detecta un sólo tipo de fenómeno físico. Cada situación en

las Unidades de Informática es diferente, la cual debe ser analizada para determinar qué dispositivo es más conveniente.

Detectores de Fuego.- Son usados en áreas de procesamiento de datos, éstos pueden ser detectores de calor o detectores de humo.

Un tipo de detector de calor es el eslabón fundible, éste se conecta a una toma de agua y se coloca en el techo del cuarto, formando un sistema de rociadores, el eslabón se derrite cuando el calor llega a ser intenso y el agua se rocía en el cuarto. El eslabón fundible y otros detectores de calor, generalmente no detectan el fuego, hasta que se haya hecho una cantidad considerable de daño.

Los detectores de humo, detectarán rápidamente el humo causado por el fuego eléctrico, éstos detectores son mucho más efectivos, pero con frecuencia dan falsas alarmas, sobre todo si la gente tiene la costumbre de fumar a los alrededores.

Apertura o Interrupción de un Circuito Eléctrico.- Estos son utilizados para detectar la apertura de una puerta específica como lo son las del almacén de registros o de una caja de conexiones telefónicas, o el rompimiento de una ventana.

En algunas aperturas se uso un micro swicht, en ventanas y algunas veces en paredes, techos y puertas se usa una cinta o alambre que

lleva corriente, si el circuito se abre, un relevador se cerrará el --- cual activa una alarma.

Circuito Eléctrico.- La presencia de un intruso puede causar -- que un micro swicht se cierre, el swicht puede estar en el panel del -- piso, en el exterior un mecanismo de swiches puede estar bajo el tapete, el intruso puede activar una luz o la energía de cuarto puede también - cerrar un circuito de alarma.

Interrupción de una luz o de un Haz Lasser.- Una luz enfocada - en un haz paralelo es enviada a través de un cuarto o un pasaje hacia - una celda fotoeléctrica, cuando el interruptor interrumpe el haz, un -- circuito de alarma se cierra, si se usa un haz de luz simple el in- - truso puede comprometer al sistema utilizando una linterna brillante sobre la celda detectora, ésto puede ser evitado usando un haz modulado, la fuente de luz y receptor están modulados por la misma frecuencia y - la sustitución de una luz diferente será detectada, el haz de luz rebota hacia y entre dos espejos, los espejos han sido usados para rodear un - objeto dentro de estos haces de luz.

Los lasser dan haces mocromáticos, los cuales tienen muy poca - dispersión y así pueden usarse en trayectorias largas para llenar un -- área grande o corredor.

Algunas ocasiones también se usan naces de luz infrarojos o ul-- travioletas.

DETECTORES DE SONIDO Y VIBRACION.- El sonido arriba de un nivel preestablecido puede activar automáticamente una alarma. Los micrófonos se usan en la superficie de una pared, ésta detectará los golpes -- que podrían indicar un intento de entrada. Los micrófonos pueden ser - utilizados únicamente en áreas tranquilas y tienden a estar sujetos a - falsas alarmas.

DETECTOR ULTRASONICO Y RADAR.- Estos dispositivos usan ondas - ultrasónicas o de radar, son utilizados para detectar movimientos den-- tro de un cuarto. Pueden ser usados para asegurar que no haya personas en el cuarto de máquinas o en una cintoteca o discoteca cuando estén ce rradas.

VARIACION EN UN CAMPO ELECTRICO.- Se utilizan para detectar la_ presencia de una persona, una persona cerca de conductor eléctrico ab-- sorbe algo de la energía en el campo y ésto opera un circuito de alar-- ma.

DETECTORES DE IMAN.- Puede usarse un detector de imán, cuando - un imán se mueva dentro de 10°ó menos alrededor de un dispositivo, acti vará un circuito de alarma.

LECTORES DE TARJETAS DE IDENTIDAD.- Este dispositivo ya fue tra tado en la Sección de Identificación del Usuario.

CIRCUITO CERRADO DE TELEVISION.- Las cámaras de televisión son_ colocadas en el cuarto del vigilante, éste fijará la imagen de la perso_ na extraña a la unidad.

DETECTORES DE ROBO.- Estos dispositivos son usados por algunas_ tiendas comerciales como se mencionó en el Capítulo I, en este caso la_ etiqueta queda permanentemente pegada a la cinta o disco y enviará una_ señal detectable cuando ésta esté siendo transportada, ésto se utiliza_ con el fin de que las cintas o discos no sean robadas o prestados para_ ser copiadas.

CAMARA CON LAPSO DE TIEMPO.- Son cámaras de cine que toman un - cuadro aproximadamente cada 30 segundos. La película cuando se revela_ puede ser repetida para ver quién estuvo en una área durante un período de tiempo determinado. Este tipo de dispositivo es el que generalmente se usa en los bancos, en las áreas de servicio al público.

6.3 Puntos Básicos que se Deben Considerar en el Diseño de la Seguridad Física

- Detección de incendios para controlar cualquier fuego_ que pudiera ocurrir.

- Detección de intrusos y la acción para atraparlos y li_ mitar los daños que pudieran hacer.

- Detección de otros problemas (por ejemplo filtraciones de agua)

- Control de entrada de empleados. La puerta puede ser desbloqueada desde la consola del vigilante, cuando un empleado se identifique, él puede ser identificado por cámaras de televisión que puedan usarse para comparar su cara con una fotografía en una tarjeta de identidad o una fotografía almacenada en la consola del vigilante.

- Control de la salida de emergencia y de los puestos del área de carga y descarga.

- Contactos con las pantallas de vigilancia (con estaciones de llave o por radio transmisión-recepción).

- Mantener una vigilancia ininterrumpida de los detectores de intrusos u otros dispositivos para que se detecte la inadecuada búsqueda del vigilante (que el vigilante se duerma o que sea corrompido).

- Detección de fallas del equipo, la requisición de ayuda del personal de mantenimiento.

- Control de evacuación de empleados en emergencias usando altavoces o sirenas de evacuación.

- Algunos sistemas de tiempo compartido trabajan sin ser atendidos, excepto durante el primer turno. En el futuro se hará más uso de computadoras más complejas que trabajan solas, excepto cuando se les da mantenimiento.

6.4 Incendios y Siniestros

La protección contra incendios debe ser de mayor interés para los directores de los centros de cómputo, especialmente cuando su instalación es esencial para el buen funcionamiento de la institución.

6.4.1 Medidas de Protección

- La elección de un sitio para minimizar cualquier cosa que se parezca a un desastre, pocos incendios se originan en un cuerto de computadora bien protegido, por lo general son inclinados a extenderse desde el exterior.

- Los ductos de aire acondicionado y otros ductos deberán ser diseñados para que no se extienda el fuego.

- Que el posicionamiento del equipo minimice los daños.

- Que no haya almacenaje de registros o artículos inflamables en el cuarto de las computadoras.

- Deben existir extinguidores contra fuego operados en forma manual y que estén disponibles en forma inmediata claramente marcados y probados periódicamente. (Figura Nº 8)

Figura Nº 8

EXTINGUIDORES DE FUEGO

- Que los extinguidores contra fuego automáticos estén en tal forma que no vayan a causar daño al equipo o que no pongan en peligro al personal. Que empiecen a funcio-- nar después de un retardo para poder permitir la intervención humana.

- Que los swiches de apagado de emergencia estén claramente marcados y que nunca estén obstruidos.

- Los procedimientos de emergencia deben de estar bien -- marcados.

  Todo el personal debe estar familiarizado con ellos y - que sepan exactamente qué hacer cuando se incie el fuego.

- Que se tomen en cuenta las medidas de seguridad al personal de los procedimientos de distribución y emergen-- cia.

- Que los registros importantes se almacenen en gabinetes o bóvedas a prueba de incendios.

- Que los registros necesarios para la reconstrucción de archivos queden almacenados fuera de las áreas de trabajo.

6.5 Instrucciones a los Operadores

Es de vital importancia que tanto los operadores como el perso-- nal que se encuentre en el cuarto de la computadora sepan qué hacer - - cuando se inicie un fuego o suene la alarma.

Es recomendable dar un entrenamiento al personal en el uso de -- extinguidores manuales, el procedimiento que se debe seguir en los ca-- sos de emergencia deberá ser colocado en un lugar visible (por ejemplo, en la pared).

6.6 Procedimientos de Apagado

El swuicht de apagado del cuarto de la computadora y el panel de energía deben estar marcados claramente y sin ninguna obstrucción. Las personas que se encuentran en el cuarto de la computadora deben ser ins truídas sobre el uso de los swuiches, el procedimiento de los swuiches_ de apagado deberá ser colocado en lugar visible. El alumbrado de la -- planta eléctrica deberá estar instalado al quitar el swuicht de apagado de emergencia, ya que pueden ser dañados ciertos equipos o registros en - los archivos.

6.7 Seguridad Personal

Un botiquín de primeros auxilios debe de estar colocado en el -- cuarto de la computadora. El instructivo de primeros auxilios deberá - ser de importancia en un programa de seguridad. El número telefónico - de algunas instituciones que presten servicios médicos (Cruz Roja, - - I M S S, I S S S T E , etc.) deberán ser colocados en lugar visible.

6.8 Sabotaje

El sabotaje es una de las amenazas más mortífera para la seguridad de la institución.

A este respecto se expresan los requerimientos mínimos necesa-- rios que un sistema de seguridad debe reunir, los cuales se encuentran_ detallados por Martín James [8]

1. El Centro de Cómputo deberá tener poca visibilidad para no lla-- mar la atención de gente de afuera, no deberán haber señales que den indicaciones de sus funciones.

---

[8] Ibid., págs. 330 y 331

2. No deberá estar en una instalación de vitrina o de aparador, si es demasiado tarde para moverse de una instalación a nivel de la planta baja de cristal, entonces - deberá revestirse con malla plástica gruesa, el fondo de vidrio deberá ser sustituido con algún otro vidrio plástico.

3. El sitio de la computadora deberá ser seleccionado pensando en la seguridad, si es posible no deberá estar a nivel de la planta baja o en el último piso del edificio. Los pisos de arriba y los de cualquier área de -- alrededor, deberán estar protegidos.
Deberá estar situado en un complejo seguro, en un edificio vigilado.

4. El equipo vital deberá estar alejado de las ventanas.

5. Cuando se planee el sitio, deberá discutirse con el arquitecto la seguridad y protección contra el sabotaje.

6. Las entradas no deberán estar en localidades obviamente vulnerables.

7. Si un velador patrulla el edificio, él deberá prestar - especial atención al centro de computación.

8. Deberán usarse alarmas contra incendios y contra intrusos, conectadas directamente a la localidad de los vigilantes o a la policía local.

9. Deberán usarse cerraduras efectivas en los alimentadores de energía para la computadora y el almacén y en los gabinetes de almacenaje. El almacenaje de cintas y discos deberá estar especialmente bien vigilado.

10. El edificio deberá tener una sola entrada, todas las personas que entren deberán ser checadas por un vigilante o una recepcionista.

11. Deberán hacerse chequeos frecuentes para que no sea posible entrar de las salidas posteriores, tales como escaleras para incendio o a través de ventanas y ventilaciones.

12. No deberá usarse la operación abierta al público.

13. Todos los visitantes deberán estar escoltados en todo momento

14. Deberán prohibirse todas las giras a través de las instalaciones.

15.- Las demostraciones para gente del exterior deberán ser evitadas si es posible, si éstas son inevitables, deberán ser rigurosamente controladas. Un cuarto de proyección ayuda a mantener alejados a los visitantes de los lugares sensibles.

16.- Los programas deberán estar rigurosamente controlados. Los métodos de control deberían prevenir de que se lleguen a usar programas no autorizados y que involucren a los archivos de datos de más importancia.

17.- Todos los jefes de las unidades deben observar cuidadosamente la moral. El personal que podría causar un daño deliberado, generalmente tiene una culpa moral sobre sus espaldas. Deberá tener cuidado especial con cualquiera que se despida.

18.- Deberá haber medios disponibles para reconstruir archivos si éstos llegan a dañarse.

19. Debe estar activo un programa de registros vitales. -- Los registros necesitados para éste y para la reconstrucción de registros generales deberán estar almacenados con seguridad y en un edificio diferente. Las personas que necesitan conocerlos, deberán estar informados de su localización.

20.- Deberá haber la disponibilidad de un Centro de Cómputo de respaldo en caso de un desastre y los programas deberán ser aprobados en este sistema.

21.- La policía local deberá estar familiarizada con la instalación e informada sobre el interés de su seguridad.

C A P I T U L O III

ANALISIS DE LOS SISTEMAS DE SEGURIDAD EN EL SECTOR PUBLICO CENTRAL

7. Desarrollo de la Investigación

7.1. Planteamiento del Problema

Para efecto de realizar el presente estudio, se muestra el si- - guiente problema:

Determinar hasta qué grado son aplicadas las normas generalmente establecidas para el control y la seguridad de los Centros de -- Cómputo en el Sector Público Central.

7.2 Hipótesis

Del problema anterior, se plantea la siguiente hipótesis:

"Sí se aplican las medidas de seguridad en los Centros de Cómputo del Sector Público Central en un 80%".

7.3 Planeación de la Investigación

Para comprobar o disprobar la hipótesis tomé como fuente de información a las Unidades de Informática del Sector Público Central, llevado a cabo las siguientes actividades:

7.4 Determinación de la Muestra

Para la realización del presente estudio y determinación de la muestra, se consideraron sólo las Unidades de Informática que tienen nivel de Dirección, teniendo un universo de 29 elementos.[9]

El Sector Público Central, se encuentra constituido actualmente por 16 Secretarías de Estado y 2 Departamentos, de esta estructura se seleccionó una Unidad de Informática por cada una de las Secretarías y Departamentos, teniendo un total de 18 elementos. Se realizó mediante la aplicación del "Muestreo a Juicio".

7.5 Elaboración del Cuestionario para las Unidades de Informática del Sector Público Central

Para la elaboración del cuestionario, se utilizaron preguntas de

---

[9] Este dato fue obtenido del "Manual de Normas y Procedimientos de Informática" Directorio de Unidades de Informática de la Administración Pública Federal. Editado por la S.P.P. Junio de 1980.

múltiple selección las cuales podían tener varias respuestas posibles, dicotómicas y tricotómicas con opción a una sola respuesta.

7.6 Prueba Piloto

Se efectuó una muestra previamente determinada para analizar las desviaciones y considerando las observaciones hechas por las personas - encuestadas, con el fin de corregir el cuestionario.

7.7 Elaboración del Cuestionario Definitivo

Una vez hechas las correcciones necesarias, se elaboró el cues-- tionario definitivo, el cual se dividió en cinco grupos de preguntas, de acuerdo al tipo de información requerida, quedando el cuestionario integrado de la siguiente manera:

I. RESPONSABILIDAD DEL SISTEMA

1.- ¿Quién es el responsable del sistema total de seguridad?

a) El Director General ( )
b) El Subdirector ( )
c) El Jefe de la Unidad de Informática ( )
d) Los Analistas de Sistemas ( )
e) Los programadores ( )

f) Los operadores ( )

g) Especialistas externos ( )

h) Ninguno ( )

i) Otros ( )

Especifique _____

_____

1 a.- ¿En quién (s) se ha (n) delegado esta responsabilidad?

a) El Director General ( )

b) El Subdirector General ( )

c) El Jefe de la Unidad de Informática ( )

d) Los analistas de sistemas ( )

e) Los programadores ( )

f) Los operadores ( )

g) Especialistas externos ( )

h) Todos los anteriores ( )

i) Ninguno ( )

j) Otros ( )

Especifique _____

_____

2.- ¿Se encuentran divididas las responsabilidades entre programadores y operadores del equipo de cómputo?

SI ( ) NO ( )

3.- ¿Existe una o varias personas que tengan las responsabilidades siguientes?

- Control y conocimiento total de los programas
- Control y conocimiento de los cambios y nuevos programas
- Revisión de los programas y especificación de los datos

SI ( ) NO ( )

II. ESTABLECIMIENTO DEL PRESUPUESTO DE SEGURIDAD

4.- ¿Se cuenta con presupuesto para cubrir las necesidades del sistema de seguridad?

SI ( ) NO ( )

NO SABE ( )

5.- ¿Cuáles de los siguientes controles de exactitud son utili- - zados en esta Unidad?

a) Verificación ( )
b) Validación ( )
c) Los dos anteriores ( )
d) Ninguno ( )
e) Otros ( )

Especifique _____

_____

6.- ¿Existen pruebas para verificar la interrelación de dos o más -- campos ¿Cuáles de las siguientes se realizan en esta Unidad?

a) Consistencia interna ( )
b) Consistencia externa ( )
c) Secuencia ( )
d) Números secuenciales ( )
e) Validez ( )
f) Todas las anteriores ( )
g) Ninguna ( )
h) Otras ( )

Especifique _____

_____

7.- Entre los controles más importantes están aquellos que prueban - integridad y precisión de un lote. ¿Se efectúan algunas de las siguientes?

a) Suma de transacciones ( )
b) Totales de control ( )
c) Los dos anteriores ( )
d) Ninguno ( )
e) Otros ( )

Especifique _____

_____

8.- De las pruebas que se realizan para asegurarse de que los programas están ejecutando correctamente las instrucciones previstas, se encuentran las pruebas durante el proceso. ¿Cuáles de éstas se llevan a cabo en la Unidad?

a) Aritméticas ( )
b) Redondeo ( )
c) Cifras de control internas ( )
d) Transacciones ficticias ( )
e) Todas las anteriores ( )

f) Ninguna ( )

g) Otras ( )

Especifique _____

_____

9.- ¿Cuáles de las pruebas de validación de salida son utilizadas en la Unidad?

a) Razonabilidad ( )

b) Números secuenciales ( )

c) Registros de cotrol ( )

d) Las tres anteriores ( )

e) Ninguna ( )

f) Otras ( )

Especifique _____

_____

10.- ¿Cuenta la Unidad con procesos en Tiempo Real?

SI ( ) NO ( )

Nota: Si la respuesta es afirmativa, continuar con la siguiente pregunta, en caso contrario, pasar a la pregunta número - 12.

11.- ¿Cuáles de los siguientes controles son utilizados en los procesos en Tiempo Real?

a) Validación de transacciones simples ( )
b) Validación de grupos de transacciones ( )
c) Los dos anteriores ( )
d) Ninguno ( )
e) Otros ( )

Especifique _____

_____

12.- ¿Existe en la Unidad Sistemas en Teleproceso?

SI ( ) NO ( )

Nota: Si la pregunta es afirmativa, continuar con la siguiente pregunta, en caso contrario, pasar a la pregunta número - 14.

13.- Para obtener exactitud en la transmisión de los datos en teleproceso, existen códigos de control. Indique cuáles son utilizados en este sistema

a) Bits de paridad ( )
b) Código estándar ASCII ( )

c) Código M-tomado-de-N (M-out-of-N) ( )

d) Todos los anteriores ( )

e) Ninguno ( )

f) Otros ( )

Especifique: _____

_____

IV. PROCEDIMIENTOS EN CASO DE FALLA DEL EQUIPO

14.- Dentro de los procesos en lote, y principalmente en aquellos que son largos, éstos son divididos en segmentos. ¿Existe esta segmentación en los procesos elaborados en esta Unidad?

SI ( ) NO ( )

14 a.- ¿Se cuentan con puntos de control al final de cada segmento?

SI ( ) NO ( )

Nota: La siguiente pregunta se deberá responder en caso de que se haya contestado afirmativamente a las preguntas números 10 y 12.

15.- ¿Cuáles de las siguientes medidas de seguridad son efectuadas en los procesos en Tiempo Real y Teleprocesos para prevenir las fallas del equipo?

a) Mensajes de recepción ( )

b) Control de numeración ( )

c) Uso de bitácoras ( )

d) Puntos de control ( )

e) Todas las anteriores ( )

f) Ninguna ( )

g) Otras ( )

Especifique _____

_____

V. RECUPERACION DE ARCHIVOS

16.- ¿Qué tipo (s) de unidades de archivo existen en los procesos en_ lote?

a) Unidades de entrada y unidades de salida (cintas o discos) ( )

b) Unidades de entrada-salida (cintas o -- discos) ( )

17.- ¿Se conservan las unidades de entrada que fueron utilizadas en - el proceso anterior?

SI ( ) NO ( )

18.- ¿Existen archivos que residan permanentemente en discos?

SI ( ) NO ( )

19.- ¿Se hacen copias totales o parciales del contenido de los archivos residentes en discos?

SI ( ) NO ( )

20.- Se conservan copias de los archivos más importantes?

SI ( ) NO ( )

VI. PRIVACIDAD DE LA INFORMACION

21.- ¿Qué tipo (s) de control (es) se utilizan para la identificación de los usuarios del sistema?

a) Por lectura de huellas digitales ( )
b) Por reconocimiento de voz ( )
c) Por medición del tamaño de los dedos ( )
d) Tecleando un código de seguridad ( )
e) Por un objeto que el usuario lleve, como una llave o una tarjeta magnética ( )
f) Todos los anteriores ( )

g) Ninguno ( )

h) Otros ( )

Especifique _____

_____

VII. SEGURIDAD FISICA

22.- ¿Qué tipo (s) de control (es) de los que a continuación se enuncian son empleados en esta unidad como protección a la seguridad física del edificio?

a) Vigilantes ( )

b) Alarmas contra intrusos ( )

c) Alarmas contra incendios ( )

d) Bóvedas ( )

e) Cuartos de almacenaje ( )

f) Cerraduras y/o candados ( )

g) Todos los anteriores ( )

h) Ninguno ( )

i) Otros ( )

Especifique _____

_____

23.- ¿Qué tipo de dispositivos de detección son utilizados en la protección física del edificio?

a) Detectores de fuego ( )
b) Detectores de imán ( )
c) Apertura o interrupción de un circuito eléctrico ( )
d) Circuito Eléctrico ( )
e) Interrupción de una luz o un haz lasser ( )
f) Detectores de sonido y vibración ( )
g) Variación de un campo eléctrico ( )
h) Detectores ultrasónicos y de radar ( )
i) Circuito cerrado de televisión ( )
j) Cámaras con lapso de tiempo ( )
k) Todos los anteriores ( )
l Ninguno ( )
ll) Otros ( )

Especifique _____

_____

Nota: Los dispositivos anteriores sirven para detectar la presencia de intrusos en una área determinada, a excepción de los dos primeros.

24.- ¿Existen en la unidad extinguidores contra fuego manuales y/o -- automáticos?

SI ( ) NO ( )

VIII. TIPOS DE EXPOSICION DE LA SEGURIDAD

25.- ¿Cuáles de las siguientes fallas han ocurrido en esta Unidad y -- con qué frecuencia?

FALLAS DE HARDWARE

a) Computador fuera de Orden

a1) Diario ( ) a3) Mensual ( ) a5) Anual ( )
a2) Semanal ( ) a4) Semenstral ( ) a6) Rara vez ( )

b) Disco u otro volumen que no se pueda leer

b1) Diario ( ) b3) Mensual ( ) b5) Anual ( )
b2) Semanal ( ) b4) Semenstral ( ) b6) Rara vez ( )

c) Error en la Transmisión de Datos por Fallas del Equipo

c1)	Diario	( )	c3)	Mensual	( )	c5)	Anual	( )
c2)	Semanal	( )	c4)	Semestral	( )	c6)	Rara vez	( )

d) Tarjetas Mutiladas por la Máquina

d1)	Diario	( )	d3)	Mensual	( )	d5)	Anual	( )
d2)	Semanal	( )	d4)	Semestral	( )	d6)	Rara vez	( )

DESCUIDOS HUMANOS

e) Error de Perforación

e1)	Diario	( )	e3)	Mensual	( )	e5)	Anual	( )
e2)	Semanal	( )	e4)	Semestral	( )	e6)	Rara vez	( )

f) Error de Entrada del Usuario a la Terminal

f1)	Diario	( )	f3)	Mensual	( )	f5)	Anual	( )
f2)	Semanal	( )	f4)	Semestral	( )	f6)	Rara vez	( )

g) Error del Operador del Computador

g1)	Diario	( )	g3)	Mensual	( )	g5)	Anual	( )
g2)	Semanal	( )	g4)	Semestral	( )	g6)	Rara vez	( )

h) Volumen Equivocado y Actualizado

h1) Diario	( )	h3) Mensual	( )	h5) Anual	( )
h2) Semanal	( )	h4) Semestral	( )	h6) Rara vez	( )

i) Cinta y Disco Extraviado

i1) Diario	( )	i3) Mensual	( )	i5) Anual	( )
i2) Semanal	( )	i4) Semestral	( )	i6) Rara vez	( )

j) Daño Físico a una Cinta o Disco

j1) Diario	( )	j3) Mensual	( )	j5) Anual	( )
j2) Semanal	( )	j4) Semestral	( )	j6) Rara vez	( )

DAÑO INTENCIONAL

k) Saqueo

k1) Diario	( )	k3) Mensual	( )	k5) Anual	( )
k2) Semanal	( )	k4) Semestral	( )	k6) Rara vez	( )

L) Sabotaje

L1)	Diario	( )	L3)	Mensual	( )	L5)	Anual	( )
L2)	Semanal	( )	L4)	Semestral	( )	L6)	Rara vez	( )

LL) Mala fe del Usuario

LL1)	Diario	( )	LL3)	Mensual	( )	LL5)	Anual	( )
LL2)	Semanal	( )	LL4)	Semestral	( )	LL6)	Rara vez	( )

m) Uso de una Terminal para Diversión

m1)	Diario	( )	m3)	Mensual	( )	m5)	Anual	( )
m2)	Semanal	( )	m4)	Semestral	( )	m6)	Rara vez	( )

n) Fraude

n1)	Diario	( )	n3)	Mensual	( )	n5)	Anual	( )
n2)	Semanal	( )	n4)	Semestral	( )	n6)	Rara vez	( )

CATASTROFES MAYORES

ñ) Fuego

ñ1)	Diario	( )	ñ3)	Mensual	( )	ñ5)	Anual	( )
ñ2)	Semanal	( )	ñ4)	Semestral	( )	ñ6)	Rara vez	( )

o) Inundación

o1)	Diario	( )	o3)	Mensual	( )	o5)	Anual ( )
o2)	Semanal	( )	o4)	Semestral	( )	o6)	Rara vez ( )

p) Otras

p1)	Diario	( )	p3)	Mensual	( )	p5)	Anual ( )
p2)	Semanal	( )	p4)	Semestral	( )	p6)	Rara vez ( )

Especifique _____

_____

7.8 Tabulación de los Datos

Debido a la facilidad en el manejo de los datos y su bajo costo de operación, se utilizó el sistema manual para su tabulación, para lo cual se siguieron los pasos que a continuación se indican:

7.8.1 Mecánica de Operación

- Contar el número de cuestionarios
- Anotar pregunta por pregunta con sus respectivas alternativas de solución
- Vaciado de la información cuestionario por cuestionario

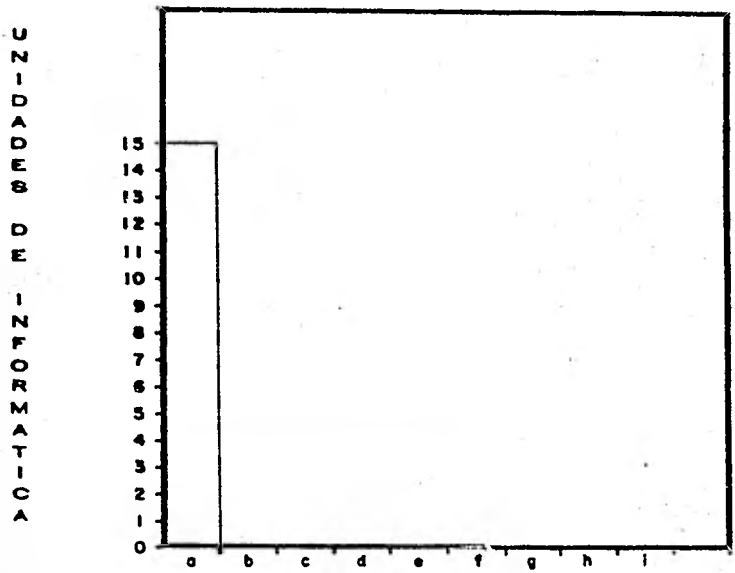
- Verificación del total de las respuestas con el total de - cuestionarios
- Totalización de los resultados por alternativa
- Determinación de los factores para la obtención de los porcentajes
- Determinación de los porcentajes por alternativa

Cabe hacer notar que de la muestra de 18 Unidades, tres de ellas - se negaron a proporcionar información, con lo cual sólo se tabularon 15_ cuestionarios.

8. REPRESENTACION GRAFICA Y PORCENTUAL DE LOS RESULTADOS OBTENIDOS

PREGUNTA 1

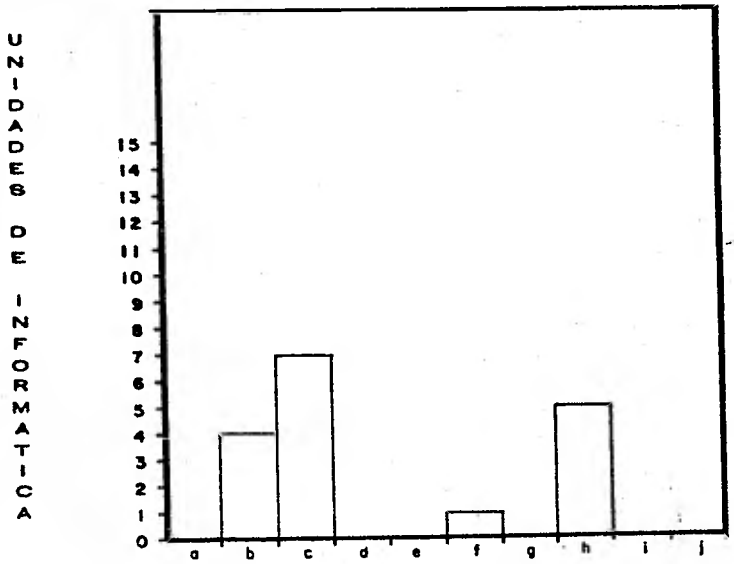
¿ QUIEN ES EL RESPONSABLE DEL SISTEMA TOTAL DE SEGURIDAD ?



ALTERNATIVAS	%
a) EL DIRECTOR GENERAL	= 100.00 %
b) EL SUBDIRECTOR	
c) EL JEFE DE LA UNIDAD DE INFORMATICA	
d) LOS ANALISTAS DE SISTEMAS	
e) LOS PROGRADORES	
f) LOS OPERADORES	
g) ESPECIALISTAS EXTERNOS	
h) NINGUNO	
i) OTROS	

PREGUNTA 1 (a)

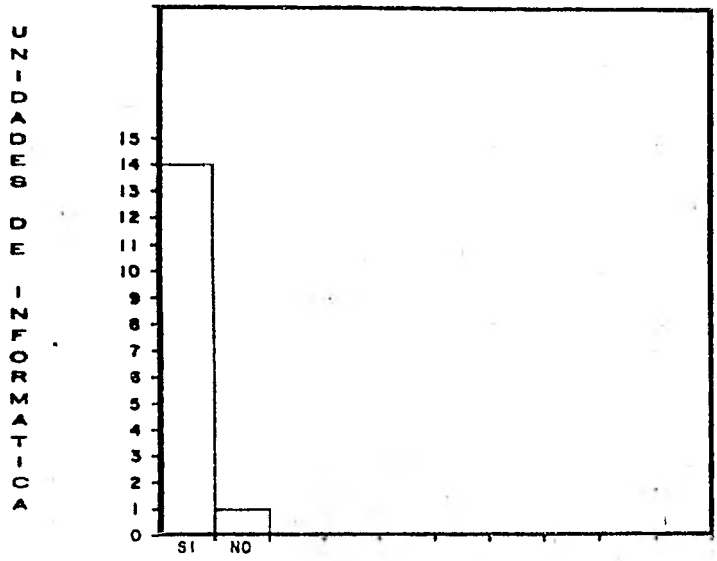
¿ EN QUIEN (ES) SE HA DELEGADO ESTA RESPONSABILIDAD ?



ALTERNATIVAS	%
a) EL DIRECTOR GENERAL	= ——
b) EL SUBDIRECTOR	= 23.529
c) EL JEFE DE LA UNIDAD DE INFORMATICA	= 41.176
d) LOS ANALISTAS DE SISTEMAS	= ——
e) LOS PROGRAMADORES	= ——
f) LOS OPERADDRES	= 5.882
g) ESPECIALISTAS EXTERNDS	= ——
h) TODOS LOS ANTERIORES	= 29.411
i) NINGUNO	= ——
j) OTROS	= ——
TOTAL	99.998 %

PREGUNTA 2

¿ SE ENCUENTRAN DIVIDIDAS LAS RESPONSABILIDADES ENTRE PROGRAMADORES Y OPERADORES DEL EQUIPO DE COMPUTO ?



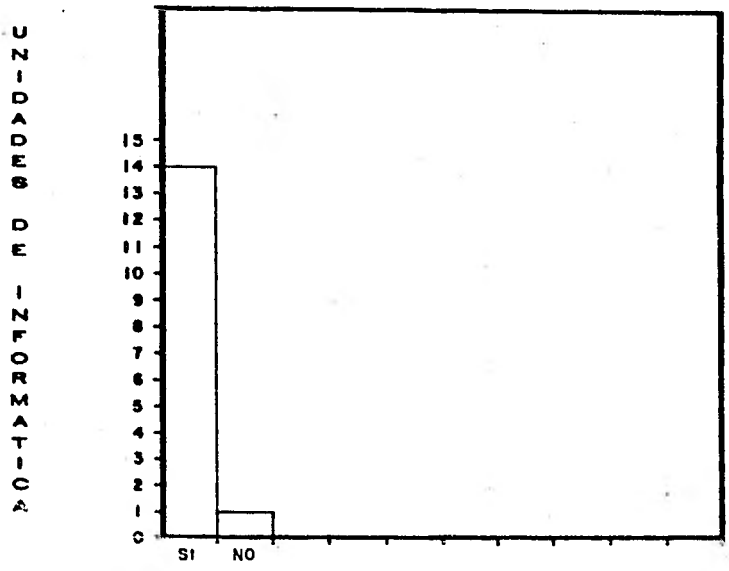
ALTERNATIVAS

	%
SI	= 93.333
NO	= 6.666
TOTAL	99.999 %

PREGUNTA 3

¿ EXISTE UNA O VARIAS PERSONAS QUE TENGAN LAS RESPONSABILIDADES SIGUIENTES ?

- CONTROL Y CONOCIMIENTO TOTAL DE LOS PROGRAMAS.
- CONTROL Y CONOCIMIENTO DE LOS CAMBIOS Y NUEVOS PROGRAMAS.
- REVISION DE LOS PROGRAMAS Y ESPECIFICACION DE LOS DATOS.

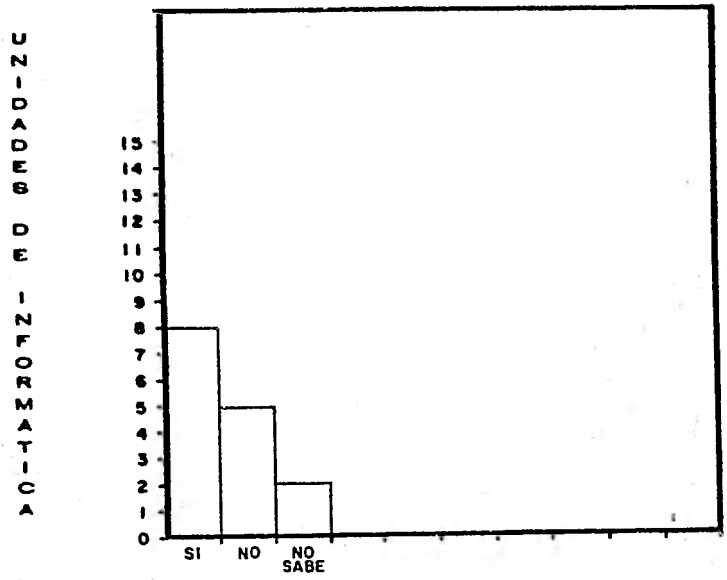


ALTERNATIVAS

	%
SI =	93 333
NO =	6.666
TOTAL	99.999 %

PREGUNTA 4

¿ SE CUENTA CON PRESUPUESTO PARA CUBRIR LAS NECESIDADES DEL SISTEMA DE SEGURIDAD ?

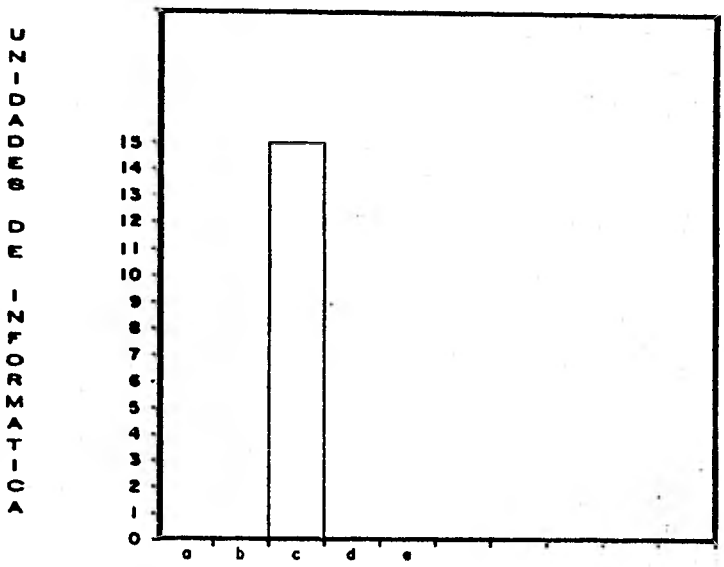


ALTERNATIVAS

	%
SI	= 53.333
NO	= 33.333
NO SABE	= 13.333
TOTAL	99.999 %

PREGUNTA 5

¿ CUALES DE LOS SIGUIENTES CONTROLES DE EXACTITUD SON UTILIZADOS EN ESTA UNIDAD ?



ALTERNATIVAS

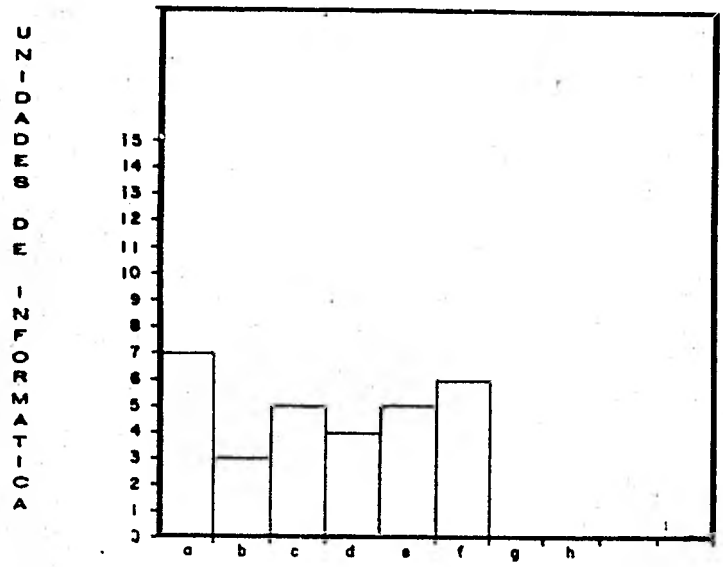
a) VERIFICACION
b) VALIDACION
c) LOS DOS ANTERIORES
b) NINGUND
e) OTROS

= 100 %

100 %

PREGUNTA 6

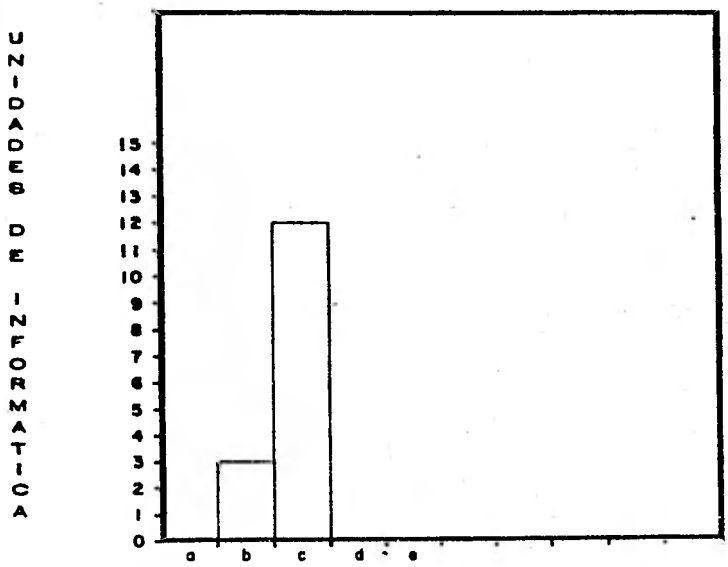
EXISTEN PRUEBAS PARA VERIFICAR LA INTERRELACION ENTRE DOS O MAS CAMPOS.
¿ CUALES DE LOS SIGUIENTES SE REALIZAN EN ESTA UNIDAD ?



ALTERNATIVAS	%
a) CONSISTENCIA INTERNA	= 23.333
b) CONSISTENCIA EXTERNA	= 10.000
c) SECUENCIA	= 16.666
d) NUMEROS SECUENCIALES	= 13.333
e) VALIDEZ	= 16.666
f) TODAS LAS ANTERIORES	= 20.000
g) NINIGUNA	
h) OTRAS	
	TOTAL 99.998 %

PREGUNTA 7

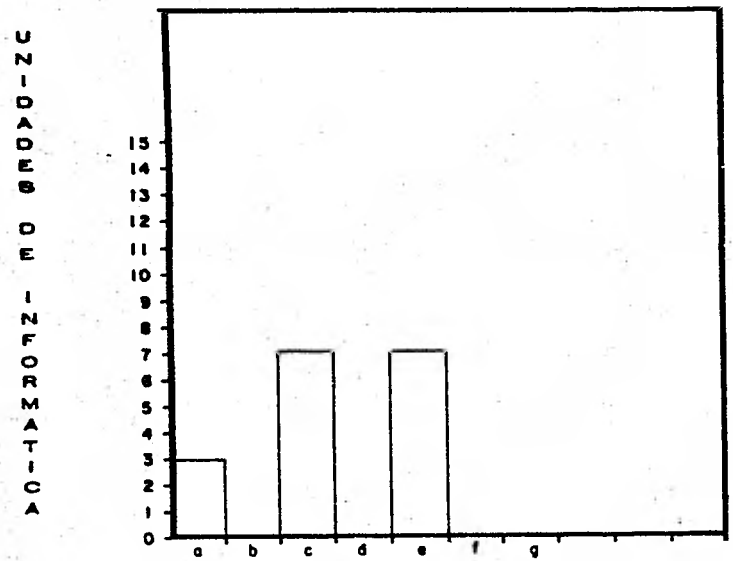
ENTRE LOS CONTROLES MAS IMPORTANTES ESTAN AQUELLOS QUE PRUEBAN LA INTEGRIDAD Y PRECISION DE UN LOTE. ¿ SE EFECTUAN ALGUNAS DE LAS SIGUIENTES ?



ALTERNATIVAS	%
a) SUMA DE TRANSACCIONES	= —
b) TOTALES DE CONTROL	= 20
c) LOS DOS ANTERIDRES	= 80
d) NINGUND	= —
e) OTROS	= —
	TOTAL 100 %

PREGUNTA 8

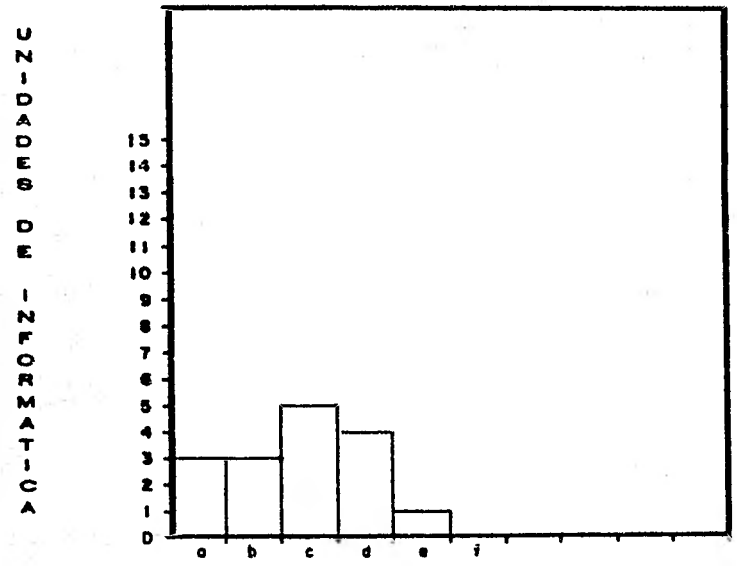
DE LAS PRUEBAS QUE SE RELIZAN PARA ASEGURARSE DE QUE LOS PROGRAMAS ESTAN EJECUTANDO CORRECTAMENTE INSTRUCCIONES PREVISTAS, SE ENCUENTRAN LAS PRUEBAS OURANTE EL PROCESO. ¿ CUALES DE ESTAS SE LLEVAN A CABO EN LA UNIDAD ?



ALTERNATIVAS	%
a) ARITMETICAS	= 17.647
b) REDONDEO	———
c) CIFRAS DE CONTROL INTERNAS	= 41.176
d) TRANSACCIONES FICTICIAS	= ———
e) TODOS LAS ANTERIORES	41.176
f) NINGUNA	= ———
g) OTRAS	= ———
	TOTAL 99.999 %

PREGUNTA 9

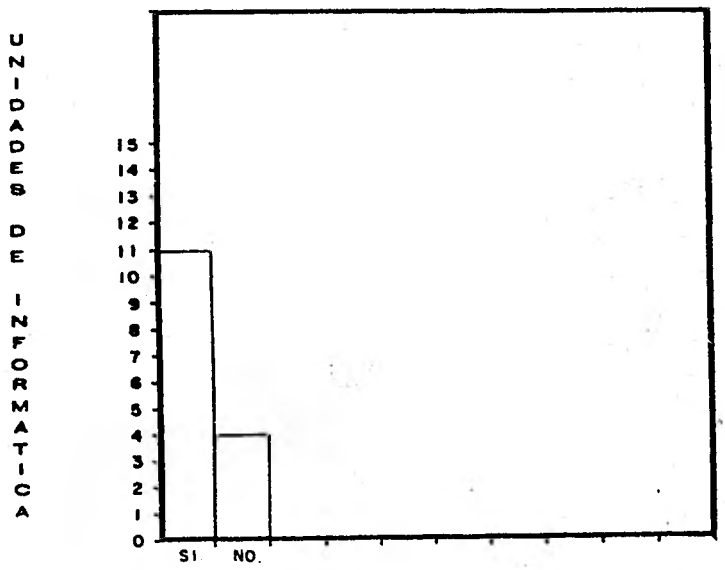
¿ CUALES DE LA PRUEBAS DE VALIDACION DE SALIDA SON UTILIZADAS EN ESTA UNIDAD ?



ALTERNATIVAS	%
a) RAZONABILIDAD	= 18.750
b) NUMEROS SECUENCIALES	= 18.750
c) REGISTROS DE CONTROL	= 31.250
d) LAS TRES ANTERIORES	= 25.000
e) NINGUNA	= 6 250
f) OTRAS	
	TOTAL 100.000 %

PREGUNTA 10

¿ CUENTA LA UNIDAD CON PROCESOS EN TIEMPO REAL ?

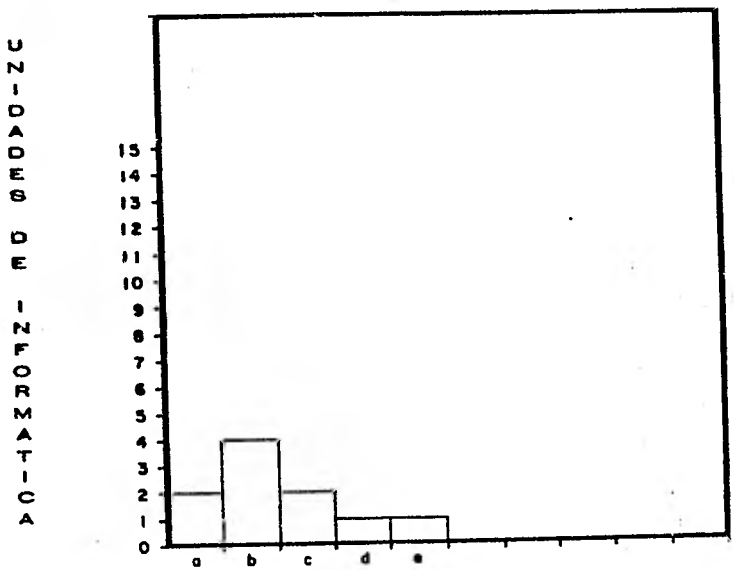


ALTERNATIVAS

	%
SI	73.333
NO	26.666
TOTAL	99.999 %

PREGUNTA 11

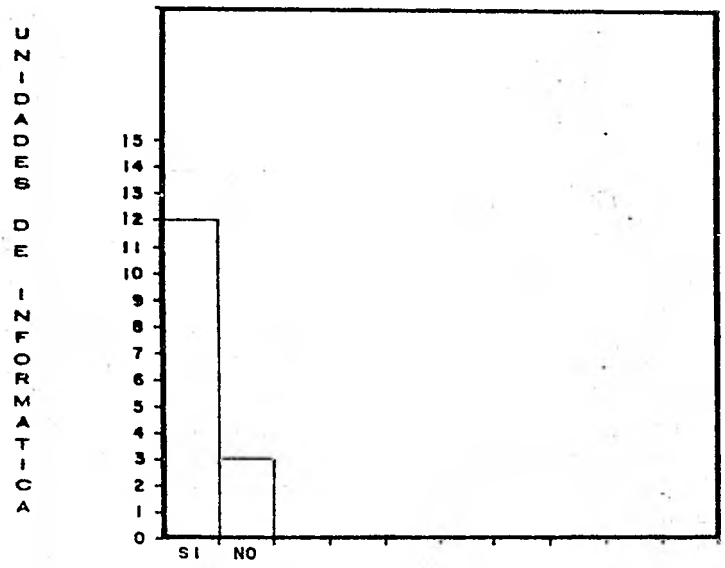
¿ CUALES DE LOS SIGUIENTES CONTROLES SON UTILIZADOS EN LOS PROCESOS EN TIEMPO REAL ?



ALTERNATIVAS	%
a) VALIDACION DE TRANSACCIONES SIMPLES	= 20
b) VALIDACION DE GRUPOS DE TRANSACCIONES	= 40
c) LOS DOS ANTERIORES	= 20
d) NINGUND	= 10
e) OTROS	= 10
	TOTAL 100 %

PREGUNTA 12

¿ EXITEN EN LA UNIDAD SISTEMAS EN TELEPROCESO ?

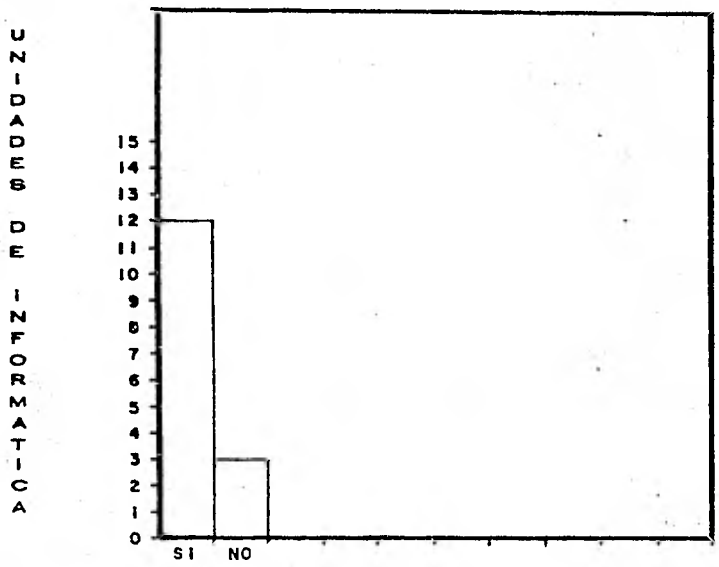


ALTERNATIVAS

	%
SI	= 80
NO	= 20
TOTAL	100 %

PREGUNTA 12

¿ EXITEN EN LA UNIDAD SISTEMAS EN TELEPROCESO ?

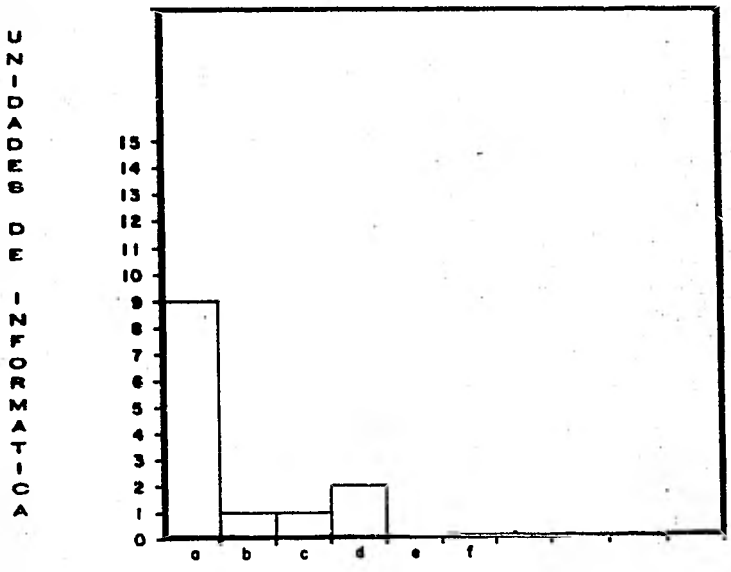


ALTERNATIVAS

	%
SI	= 80
NO	= 20
TOTAL	100 %

PREGUNTA 13

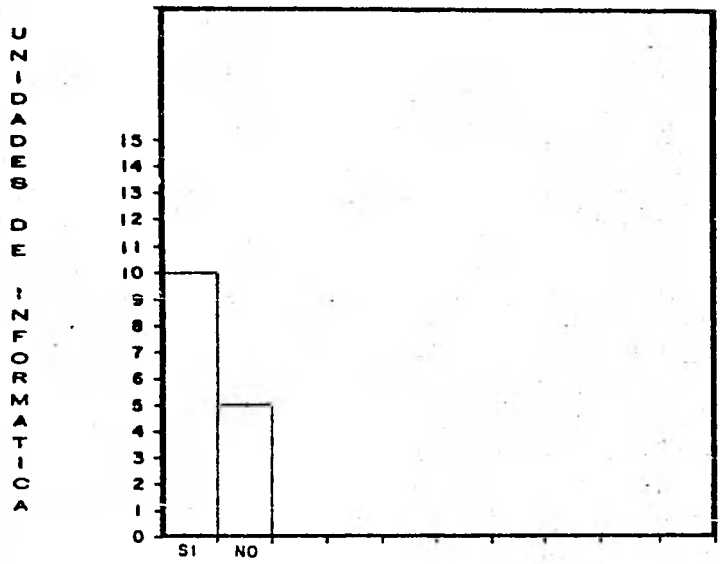
PARA OBTENER EXACTITUD EN LA TRANSMISION DE LOS DATOS EN TELEPROCESO EXITEN CODIGOS DE CONTROL. ¿ INDIQUE CUALES SON UTILIZADOS EN ESTE SISTEMA ?



ALTERNATIVAS	%
a) BITS DE PARIDAD	= 69.230
b) CODIGO ESTANDAR A.S.C.I.I.	= 7.692
c) CODIGO M-TOMADOS DE N (M-OUT-OF-N)	= 7.692
d) TODOS LOS ANTERIORES	= 15.384
e) NINGUNO	= ——
f) OTROS	= ——
	TOTAL 99.998 %

PREGUNTA 14 (a)

¿ SE CUENTAN CON PUNTOS DE CONTROL AL FINAL DE CADA SEGMENTO ?

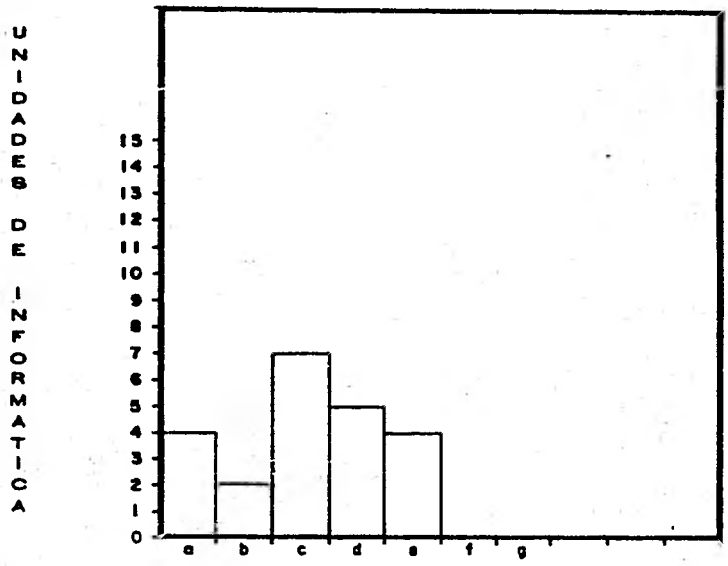


ALTERNATIVAS

	%
SI =	66.666
NO =	33.333
TOTAL	99.999 %

PREGUNTA 15

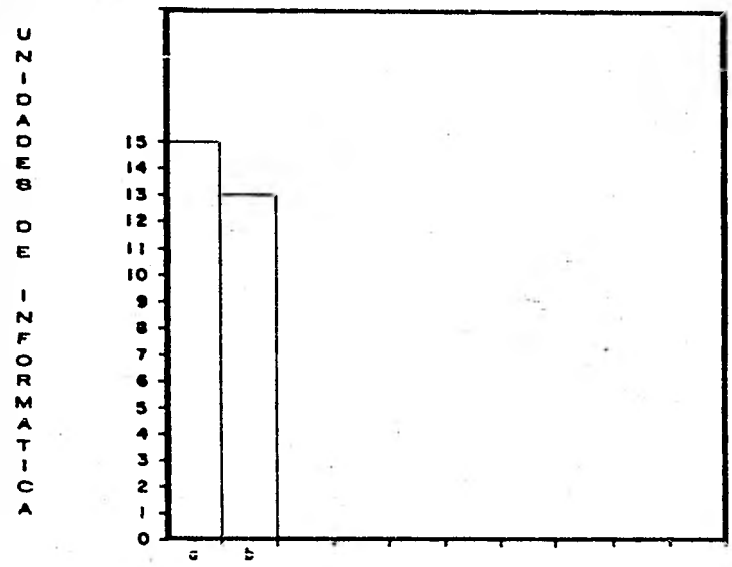
¿ CUALES DE LAS SIGUIENTES MEDIDAS DE SEGURIDAD SON EFECTUADAS EN LOS PROCESOS EN TIEMPO REAL Y/O TELEPROCESO PARA PREVENIR LAS FALLAS OEL EQUIPO ?



ALTERNATIVAS	%
a) MENSAJES DE RECEPCION	= 18.181
b) CONTROL DE NUMERACION	= 9.090
c) USO OE BITACORAS	= 31.813
d) PUNTOS DE CONTROL	= 22.727
e) TODOS LOS ANTERIORES	= 18.181
f) NINGUNO	——
g) OTROS	——
	TOTAL 99.997 %

PREGUNTA 16

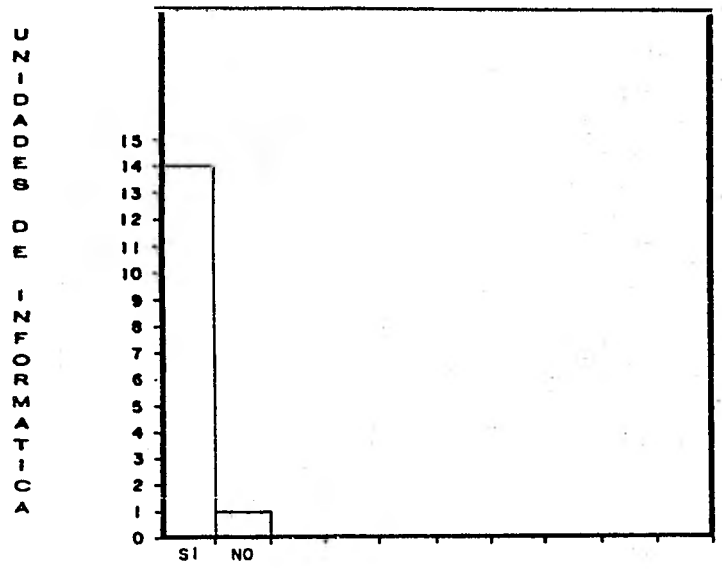
¿ QUE TIPO (S) DE UNIDADES DE ARCHIVO EXISTEN EN LOS PROCESOS EN LOTE ?



ALTERNATIVAS	%
a) UNIDADES DE ENTRADA Y UNIDADES DE SALIDA (CINTAS O DISCOS)	= 53 571
b) UNIDADES DE ENTRADA - SALIDA (CINTAS O DISCOS)	= 46 428
TOTAL	99.999 %

PREGUNTA 17

¿ SE CONSERVAN LAS UNIDADES DE ENTRADA QUE FUERON UTILIZADAS EN EL PROCESO ANTERIOR ?

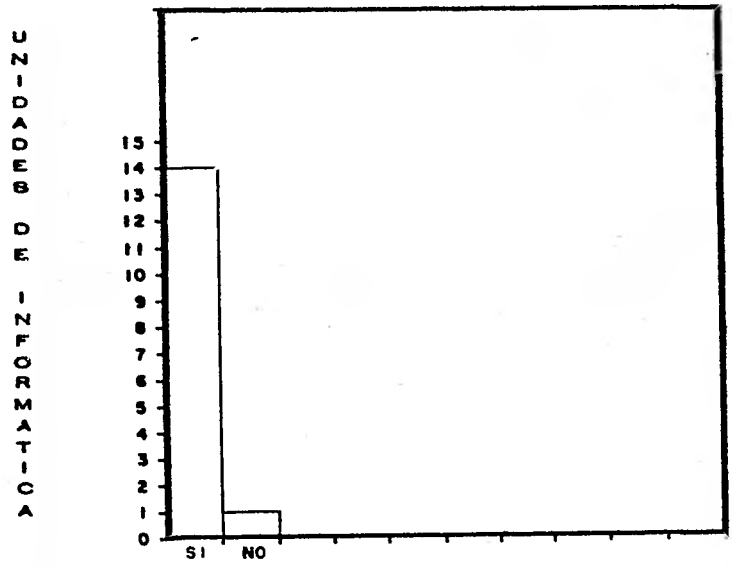


ALTERNATIVAS

	%
SI	93.333
NO	6.666
TOTAL	99.999 %

PREGUNTA 18

¿ EXISTEN ARCHIVOS QUE RESIDAN PERMANENTEMENTE EN DISCOS ?

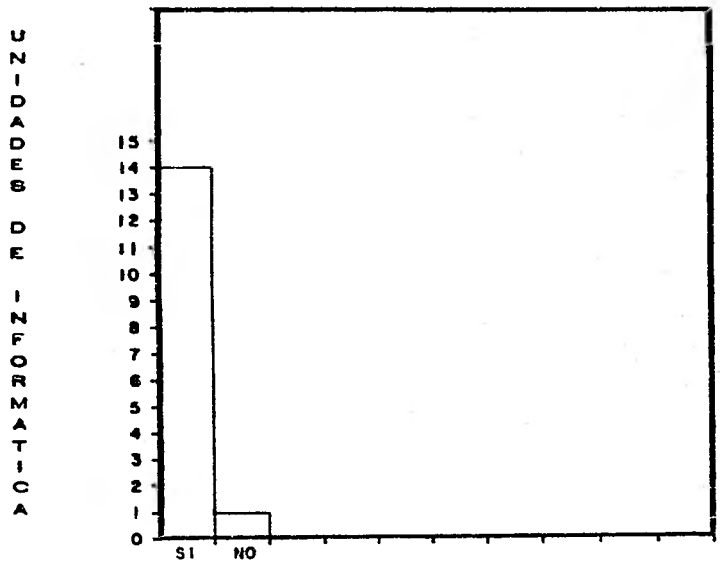


ALTERNATIVAS

	%
SI	93:333
NO	6.666
TOTAL	99.999 %

PREGUNTA 19

¿ SE HACEN COPIAS TOTALES O PARCIALES DEL CONTENIDO DE LOS ARCHIVOS RESIDENTES EN DISCOS ?

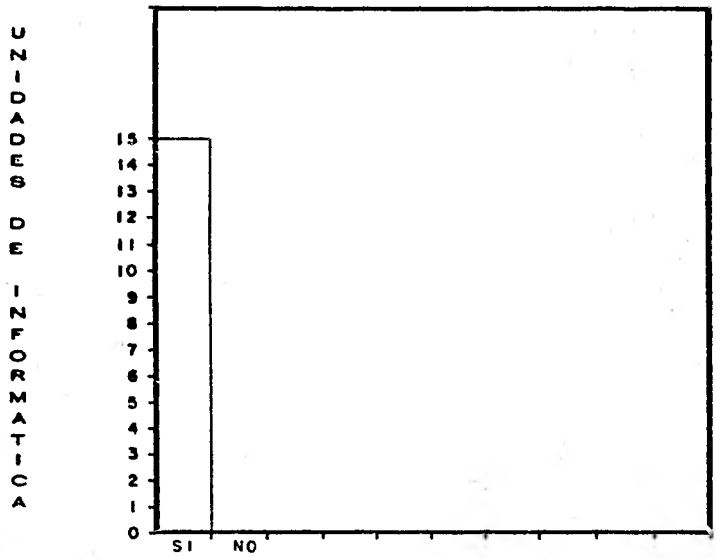


ALTERNATIVAS

	%
SI =	93.333
NO =	6.666
TOTAL	99.999 %

PREGUNTA 20

¿ SE CONSERVAN COPIAS DE LOS ARCHIVOS MAS IMPORTANTES ?

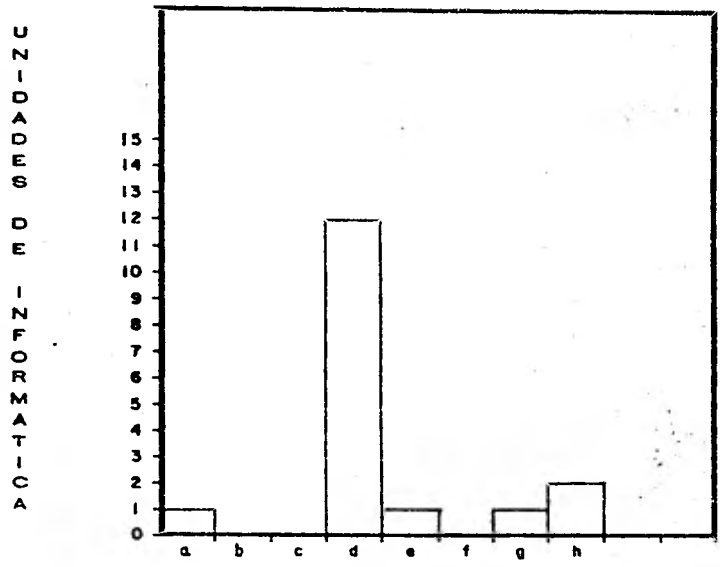


ALTERNATIVAS

SI = 100 %
NO = ——

PREGUNTA 21

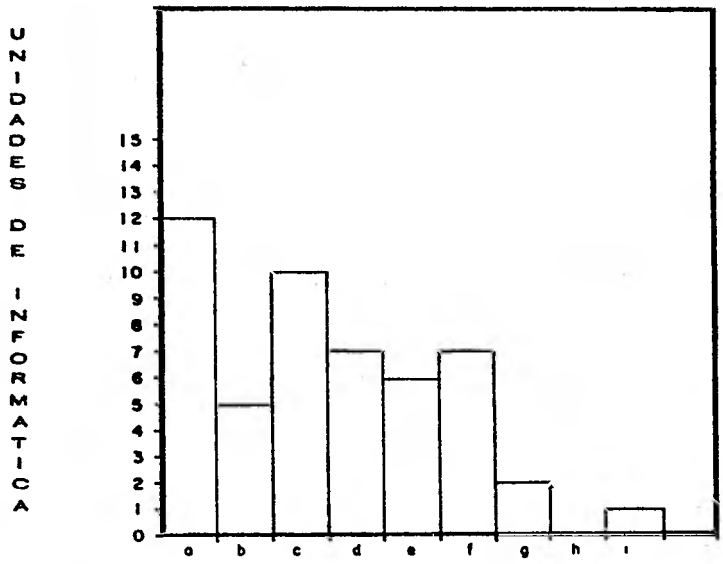
¿ QUE TIPO(S) DE CONTROL SE UTILIZAN PARA LA INDENTIFICACION DE LOS USUARIOS AL SISTEMA ?



		%
a) POR LA LECTURA DE HUELLA DIGITALES	=	5 882
b) POR RECONOCIMIENTO DE VOZ		——
c) POR MEDICION DEL TAMAÑO DE LOS DEDOS	=	——
d) TECLEANDO UN CODIGO DE SEGURIDAD	=	70.588
e) POR UN OBJETO QUE EL USUARIO LLEVE, COMO UNA LLAVE O TARJETA MAGNETICA	=	5.882
f) TODOS LOS ANTERIORES	=	——
g) NINGUNA	=	5.882
h) OTROS		11.764
	TOTAL	99 998 %

PREGUNTA 22

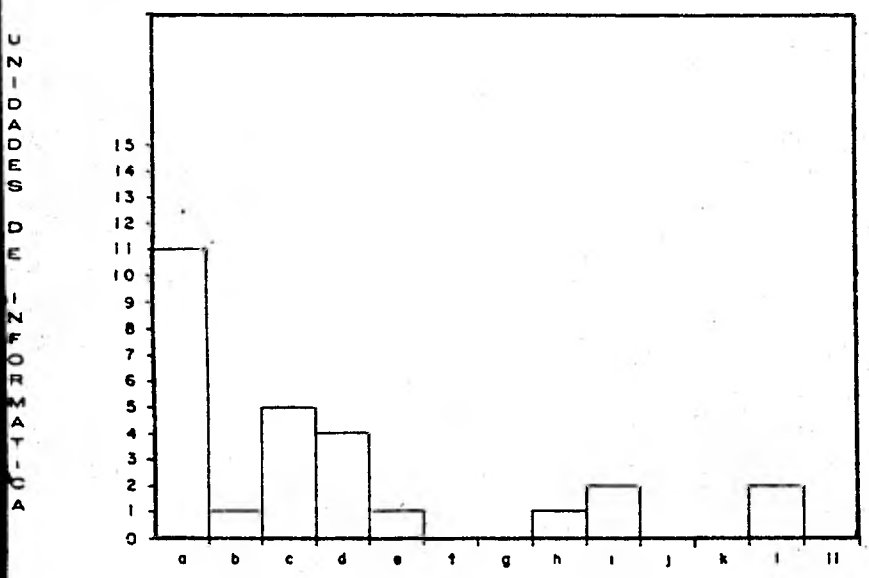
¿ QUE TIPO(S) DE CONTROL DE LOS QUE ACONTINUACION SE ENUNCIA SON EMPLEADOS EN ESTA UNIDAD COMO PROTECCION A LA SEGURIDAD FISICA DEL EDIFICIO ?



ALTENATIVAS		%
a) VIGILANTES	=	24
b) ALARMAS CONTRA INTRUSOS	=	10
c) ALARMAS CONTRA INCENDIOS	=	20
d) BOVEDA	=	14
e) CUARTOS DE ALMACENAJE	=	12
f) CERRADURAS Y/O CANDADOS	=	14
g) TODOS LOS ANTERIORES	=	4
h) NINGUNO	=	—
i) OTROS	=	2
TOTAL		%

PREGUNTA 23

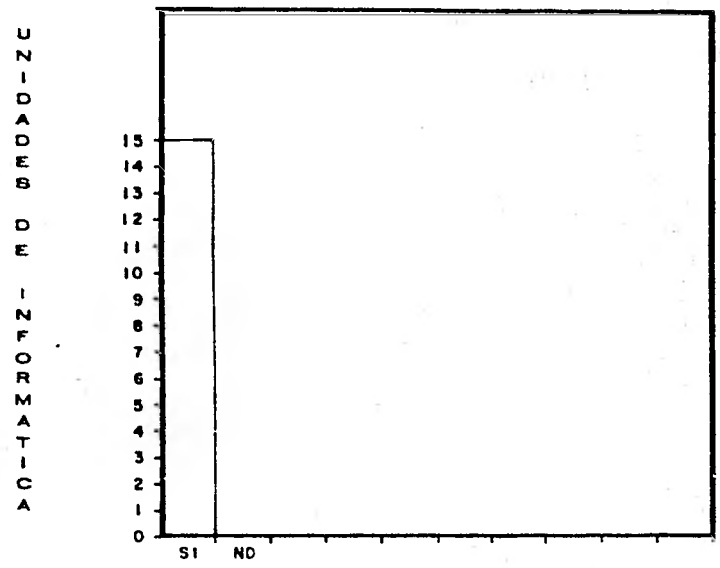
¿ QUE TIPO(S) DE DISPOSITIVOS DE DETECCION SON UTILIZADOS EN LA PROTECCION FISICA DEL EDIFICIO ?



ALTERNATIVAS	%
a) DETECTORES DE FUEGO	= 40 740
b) DETECTORES DE IMAN	= 3.703
c) APERTURA O INTERRUPCION DE UN CIRCUITO ELECTRICO	= 18 518
d) CIRCUITO ELECTRICO	= 14.814
e) INTERRUPCION DE UNA LUZ O HAZ LASSER	= 3 703
f) DETECTORES DE SONIDO Y VIBRACION	= ——
g) VARIACION DE UN CAMPO ELECTRICO	= ——
h) DETECTORES ULTRASONICOS Y DE RADAR	= 3 703
i) CIRCUITO CERRADO DE TELEVISION	= 7.407
j) CAMARAS CON LAPSO DE TIEMPO	= ——
k) TODOS LOS ANTERIORES	= ——
l) NINGUNO	= 7 407
ll) OTROS	= ——
	TOTAL 99 995 %

PREGUNTA 24

¿ EXITEN EN LA UNIDAD EXTINGUIDDS CONTRA FUEGO MANUALES Y/O AUTOMATICOS ?

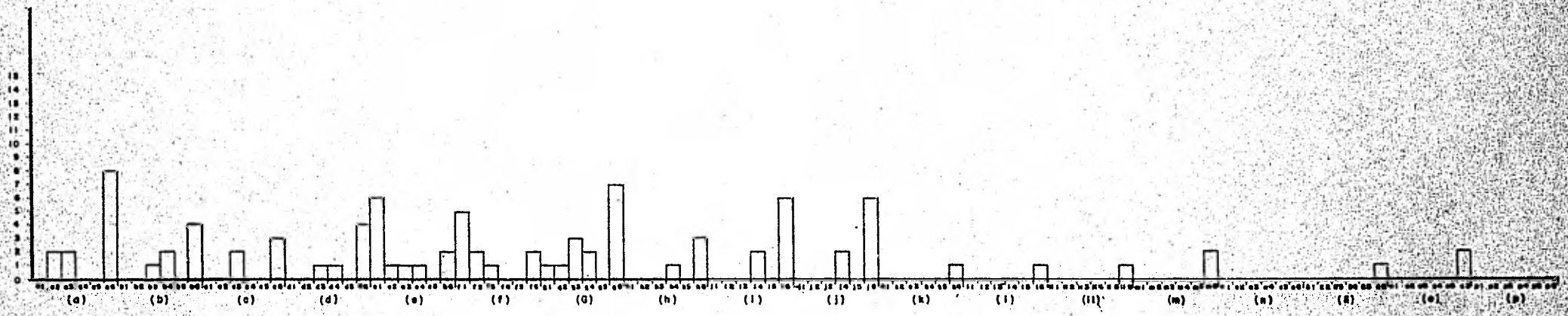


ALTERNATIVAS

SI : 100 %
NO : ——

REGUNTA 25

ALES DE LAS SIGUIENTES FALLAS HAN OCURRIDO EN ESTA UNIDAD Y CON QUE FRECUENCIA ?



PREGUNTA No. 25

Representación Porcentual:

a) Computador fuera de orden

a1) Diario		a3) Mensual	= 2.150%	a5) Anual	
a2) Semanal	= 2.150%	a4) Semestral		a6) Rara vez =	8.602%
	2.150%		2.150%		8.602%
				Subtotal:	= 12.902%

b) Disco u otro volumen que no se pueda leer

b1) Diario		b3) Mensual	= 1.075%	b5) Anual	
b2) Semanal		b4) Semestral	= 2.150%	b6) Rara vez =	4.301%
			3.225%		4.301%
				Subtotal:	= 7.526%

c) Error en la Transmisión de los datos por fallas del equipo

c1) Diario		c3) Mensual	= 2.150%	c5) Anual	
c2) Semanal		c4) Semestral		c6) Rara vez =	3.225%
			2.150%		3.225%
				Subtotal:	5.375%

d) Tarjetas mutiladas por la máquina

d1) Diario		d3) Mensual	= 1.075%	d5) Anual	
d2) Semanal		d4) Semestral	= 1.075	d6) Rara vez	= 4.301%
			2.150%		4.301%
				Subtotal:	6.451%

e) Error de perforación

e1) Diario	= 6.451%	e3) Mensual	= 1.075%	e5) Anual	
e2) Semanal	= 1.075	e4) Semestral	= 1.075	e6) Rara vez	= 2.150%
	7.526%		2.150%		2.150%
				Subtotal:	11.826%

f) Error de entrada del usuario a la Terminal

f1) Diario	= 5.376%	f3) Mensual	= 1.075%	f5) Anual	
f2) Semanal	= 2.150	f4) Semestral		f6) Rara vez	= 2.150%
	7.526%		1.075%		2.150%
				Subtotal:	10.751%

g) Error del operador del computador

g1) Diario	= 1.075%	g3) Mensual	= 3.225%	g5) Anual	
g2) Semanal	= 1.075	g4) Semestral	= 2.150	g6) Rara vez	= 7.526%
	2.150%		5.375%		7.526%
				Subtotal:	15.051%

h) Volumen equivocado y actualizado

h1) Diario	h3) Mensual		h5) Anual	
h2) Semanal	h4) Semestral	= 1.075%	h6) Rara vez =	3.225%
		1.075%		3.225%
			Subtotal:	4.300%

i) Cintas o disco extraviado

i1) Diario	i3) Mensual		i5) Anual	
i2) Semanal	i4) Semestral	= 2.150%	i6) Rara vez =	6.451%
		2.150%		6.451%
			Subtotal:	8.601%

j) Daño físico a una cinta o disco

j1) Diario	j3) Mensual		j5) Anual	
j2) Semanal	j4) Semestral	= 2.150%	j6) Rara vez =	6.451%
		2.150%		6.451%
			Subtotal:	8.601%

k) Saqueo

k1) Diario	k3) Mensual		k5) Anual	
k2) Semanal	k4) Semestral		k6) Rara Vez =	1.075%
				1.075%
			Subtotal:	1.075%

l) Sabotaje

11) Diario	13) Mensual	15) Anual	
12) Semanal	14) Semestral	16) Rara vez =	1.075%
			1.075%
		Subtotal:	1.075%

11) Mala fé del usuario

111)Diario	113)Mensual	115)Anual	
112)Semanal	114)Semestral	116)Rara vez =	1.075%
			1.075%
		Subtotal:	1.075%

m) Uso de una Terminal para diversión

m1) Diario	m3) Mensual	m5) Anual	
m2) Semanal	m4) Semestral	m6) Rara vez =	2.150%
			2.150%
		Subtotal:	2.150%

n) Fraude

n1) Diario	n3) Mensual	n5) Anual
n2) Semanal	n4) Semestral	n6) Rara vez

ñ) Fuego

ñ1) Diario	ñ3) Mensual	ñ5) Anual	
ñ2) Semanal	ñ4) Semestral	ñ6) Rara vez =	1.075%
			1.075%
		Subtotal:	1.075%

o) Inundación

o1) Diario	o3) Mensual	o5) Anual	
o2) Semanal	o4) Semestral	o6) Rara vez =	2.150%
			2.150%
		Subtotal:	2.150%

p) Otros

p1) Diario	p3) Mensual	p5) Anual
p2) Semanal	p4) Semestral	p6) Rara vez

SUMA DE SUBTOTALES:
(Porciento)

a)	12.902
b)	7.526
c)	5.375
d)	6.451
e)	11.826
f)	10.751
g)	15.051
h)	4.300
i)	8.601
j)	8.601
k)	1.075
l)	1.075
ll)	1.075
m)	2.150
n)	---
ñ)	1.075
o)	2.150
p)	---
TOTAL	99.984 %

9. Interpretación de los Datos

Para la interpretación de los datos se tomó en consideración la -- agrupación de las preguntas tal como fueron planteadas en el cuestiona-- rio, la cual es la siguiente:

I. Responsabilidad del sistema (preguntas 1 a 3)

II. Establecimiento del presupuesto de seguridad (pregunta 4)

III. Controles necesarios para la exactitud de la información - (preguntas 5 a 13)

IV. Procedimientos en caso de falla del equipo (preguntas 14 y 15)

V. Recuperación de Archivos (preguntas 16 a 20)

VI. Privacidad de la información (pregunta 21)

VII. Seguridad física (preguntas 22 a 24)

VIII. Tipos de exposición de la seguridad (pregunta 25)

Para las preguntas del grupo número I, se obtuvieron los siguientes resultados:

Pregunta 1.- Se tiene que en todas las unidades el responsable del sistema total de seguridad es el Director General, ésto es aceptable pues es la Dirección quien debe ser la responsable directa.

Pregunta 1a.- Sólo el 29.411% de las personas entrevistadas respondió que todos tienen responsabilidad en alguna parte del sistema, ésto es lo ideal dentro de la delegación de funciones pues nos da un mayor índice de seguridad al encontrarse dispersas, el 70.589% restante, contestó que se tenía responsabilidad en el sistema, pero no se encontraban involucradas todas las personas que en una forma u otra tienen contacto con la computadora.

Esto resulta contradictorio con la respuesta que se dió en la pregunta número 2, en la cual se preguntaba si se encontraban divididas las responsabilidades entre programadores y operadores, el 93.333%, respondió que sí se tienen distribuidas.

Por lo anterior, se deduce que no saben exactamente cuál es el grado de responsabilidad que deben tener las personas que intervienen en el sistema.

Pregunta 3.- De las quince personas a las que se les acplicó el cuestionario, el 93.333% objetó que sí existe una persona o un grupo -- que tenga la responsabilidad de controlar los programas, ésto resulta - bastante favorable, porque de esta manera se mejora el sistema de seguridad, revisando el trabajo de los programadores evitando cualquier modificación o cambio no autorizado a los programas e inclusive cualquier intento de fraude.

Pregunta 4.- La cual representa el segundo grupo; se tiene que - el 53.333% de las unidades cuentan con presupuesto para sus programas - de seguridad, el 33.333% no cuenta con presupuesto y el el 13.333% no - sabe si existe, ésto significa que no se han preocupado por establecer el costo que se requiere para proteger su información contra revelaciones y modificaciones no autorizadas y destrucciones, así como del esta-- blecimiento del costo para la protección física del Centro, denotando - además, una mala organización en este aspecto, puesto que no se establecen programas para el cumplimiento más eficiente de sus objetivos.

Para el grupo III de preguntas se obtuvieron los siguientes resultados:

La respuesta única que se dió por todas las Unidades de Informática en la pregunta número 5, nos da a entender que la información que se captura tiene un mínimo de errores, ya que toda es verificada y/o validada, ésto se debe básicamente a que existen las Unidades Verificadoras in

tegradas al sistema, o bien los datos van siendo validados por un pro-- grama automáticamente.

En la pregunta número 6, sólo el 20% de las Unidades realizan todas las pruebas, ésto les da un mayor índice de seguridad, el porcentaje restante se encuentra distribuido de la siguiente manera:

Consistencia interna 23.333%; Consistencia externa 10%,, Secuencia 16.666%; Números secuenciales 13.333% y Validez 16.666%. Esto no -- quiere decir que no sean seguros, ya que dependen del tipo de aplicaciones y procesos que utilicen.

Como se puede observar en la pregunta número 7, el 80% de las Unidades, se lleva a cabo tanto el control de sumas de transacciones, como el total de control, aunque estas pruebas pueden ser complementarias, el 20% respondió que sólo se realizaba el segundo tipo de control, resul-- tando en general seguro la integración y precisión de los lotes aun - - cuando sean omitidos cualquiera de estos tipos de control.

Se obtuvieron los siguientes resultados en la pregunta 8: el - - 41.176% de las Unidades realizan todas las pruebas para verificar que - los programadores ejecuten todas las instrucciones previstas, ésto da - un mayor grado de seguridad, el porcentaje restante se encuentra distribuido de tal manera que los Centros de Cómputo a los que se aplicó el -- cuestionario, sólo efectúan alguna o algunas de las pruebas que se men--

cionan, sin dejar de ser seguros, ya que ésto está supeditado al tipo - de aplicación y proceso que se esté utilizando.

Las pruebas de validación de salida resultan sumamente importan-- tantes, sin embargo, en la pregunta número 9 se llegó a responder - - - (el 6.250%) que no se efectuaban ninguna de estas pruebas, el porcentaje mayor se ubicó en los registros de salida que fue del 31.250%, siendo - el control más importante, porque es en éste donde se graban las etiquetas de control que toda corrida debe llevar, el 25% indicó que se efectuaban los tres tipos de prueba a que se hizo referencia, (razonabilidad, números secuenciales y registros de control), siendo éste el por-- centaje de mayor índice de seguridad, en razonabilidad y números secuenciales se registró el 18.750%, para cada una de estas alternativas, considerando estas pruebas de importancia, pero se encuentran sujetas al - tipo de aplicación y proceso que se utilice.

Las preguntas 10 y 12, fueron de control para poder proseguir con las preguntas correspondientes, pero ambas, en cierta forma, se encuentran interrelacionadas, por un lado se preguntó si se contaba con procesos en Tiempo Real, de las cuales el 73.333% (11 unidades), afirmaron - que sí lo tienen, por otra parte, se preguntó si existían sistemas en - teleproceso en la que se registró que el 80% (12 unidades), cuenta con él, ésto significa que 11 Unidades pueden estar procesando su informa-- ción desde varias terminales con acceso directo e instantáneo, desde lugares remotos, y una Unidad más. cuenta con terminales desde luga--

res remotos, pero sin tener acceso directo e instantáneo.

Pregunta 11.- El 20% de las Unidades argumentó que se realizaba tanto la validación de transacciones simples, como las de grupo de transacciones, estos controles tienen mayor importancia, debido a que existen varios usuarios diseminados en distintos lugares alimentando simultáneamente información, por lo cual el porcentaje resulta bajo para tener un grado de seguridad aceptable, un 20% manifestó que sólo se efectuaba el primer control y un 40% el segundo, un 10% informó que no llevaban ningún control, con lo cual se nota que no se han preocupado por establecer estos tipos de controles tan esenciales para la transmisión de datos, aunque un 10% más expresó que se utilizaban otros tipos de controles.

El porcentaje más elevando denotado en la pregunta 13, se encuentra en la opción Bits de paridad que es del 69.230%, para el Código Es-Estándar ASCII se tiene un 7.692% y para el código M-tomado-de N - - -- (M-out-of-N), se tiene 7.692% y el 15.384% para todos los anteriores, - ésto significa que sí existe seguridad, a ésto se auna el hecho de que la selección del código no afecta mayormente el rendimiento del sistema, ya que este problema lo resuelven mediante el uso de modelos de alta velocidad y/o con adisiones de más líneas de comunicación.

Los resultados obtenidos en el grupo IV. Procedimientos en Caso de Falla de Equipo, son los siguientes:

Para las preguntas 14 y 14a, el 66.666% expresó que se segmentaban los procesos largos y además que se contaban con puntos de control al_ final de cada uno de éstos. ésto nos da a entender que la mayoría toma en cuenta esta medida para no tener que reiniciar un proceso largo, des de el inicio, sino sólo a partir del punto donde halla ocurrido la fa-- lla.

Pregunta 15.- El 18.181% declaró que se efectuaban todas las prue bas para la prevención de fallas del equipo en los procesos en Tiempo -- Real y/o Teleproceso, ésto nos da un mayor grado de seguridad, aunque el porcentaje restante se encuentra distribuido en los demás controles, no quiere decir que no sean seguros, puesto que depende de las aplicacio-- nes que se realicen.

Los resultados obtenidos del grupo V, son los siguientes:

Las preguntas 16 y 17, se encuentran estrechamente relacionadas - por una parte, se tiene que las 15 Unidades donde fue aplicado el cues- tionario, cuentan con archivos de entrada y de salida para sus procesos en lote y por otro lado, 14 Dependencias conservan sus archivos del pro ceso anterior, ésto les proporciona una seguridad adicional, porque les permite aplicar la técnica del "abuelo-padre-hijo".

La pregunta 18 fue de control, la cual nos da la pauta para con tinuar con la pregunta 19, las cuales se encuentran íntimamente relacio-

nadas, el 93.333% (14 Unidades), cuentan con archivos que residen permanentemente en discos, de los cuales se hacen copias totales y/o parciales, lo anterior hace suponer que se han tomado las medidas necesarias para la reconstrucción de este tipo de archivos.

La información lograda en la pregunta 20, fue que el total de las Unidades conservan copias de los archivos más importantes, ésto nos --- muestra que sí se cuenta con los controles necesarios para poder disponer en cualquier momento de una copia, en caso de que por alguna falla no se pueda tener acceso al archivo original.

El grupo VI. Privacidad de la Información, se encuentra integrado con la pregunta 21, la cual muestra lo siguiente:

- El porcentaje mayor se encuentra en el inciso (d) tecleando un código de seguridad = 70.588%; los incisos (a), por la lectura de huellas digitales y (e), por un objeto que el usuario lleve, como una llave o tarjeta magnética= - -- 5.882% por cada alternativa.

- Otro tipo de controles= 11.764%

- Con el 5.882%, no se lleva ningún control

Este último porcentaje resulta un tanto cuanto ilógico, ya que para acceder a cualquier tipo de sistema, se debe contar al menos con una clave para poder hacerlo, con lo que respecta a los demás porcentajes,- es aceptable, debido a que el tipo de control utilizado depende del tipo de proceso que se utilice sin dejar de ser inseguro en uno u otro -- caso.

Para las preguntas del grupo VII. Seguridad Física, se tiene lo_ siguiente:

En la pregunta 22, sólo el 4% de Unidades afirmaron que contaban_ con todos los controles enunciados como protección a la seguridad física del edificio, ésto es un bajo índice, ya que lo más recomendable es_ que cuente con todos ellos, el 96% restante, utiliza sólo alguno o algunos de estos controles, siendo importantes todos, cada uno en el aspecto para lo cual han sido diseñados.

Para la pregunta número 23, el porcentaje más alto fue indicado - en los detectores de fuego que fue del 40.740%, dicho porcentaje resulta bajo, ya que al menos todas las Unidades deberían de contar con este tipo de detector tan necesario, sólo una Unidad cuenta con detectores - de imán, a este respecto la mayoría desconocía que existienra este tipo de detectores, las alternativas de la (c) a la (s), se refieren a detectores para captar la presencia de un intruso en el Centro de Cómputo o_ en áreas cercanas a éste. En este sentido, el 48.145%, señaló que con-

taban con alguno de estos dispositivos, resultando también bajo el porcentaje, ya que todas las Unidades debieran contar al menos con cualquiera de estos aparatos, un 7.407% afirmó que no contaban con ningún tipo de dispositivos, ésto confirma que no se ha dado la dibida importancia a la seguridad física del edificio.

El total de las Unidades manifestó que contaban con extinguidores de fuego, los cuales son esenciales en cualquier organización (pregunta 24).

El último grupo "Tipos de Exposición de la Seguridad", se hizo una sola pregunta referente al tipo de fallas que hayan ocurrido en el Centro y con qué frecuencia, para su tabulación y análisis se dividió en 13 incisos, de la (a) a la (p) y éstos a su vez se subdividieron en 6 subincisos para poder determinar la frecuencia. La finalidad de esta pregunta fue confirmar el grado de seguridad de los Centros, a través de las fallas ocurridas a éstos. Los parámetros que se fijaron para poder determinar en qué aspecto afecta a la información los errores que se pueden presentar son los siguientes:

- Incapacidad para procesar
- Pérdida de un archivo completo
- Pérdida de registros simples
- Modificación de registros.
- Lectura o copia no autorizada

Al final de esta sección, se presenta una matríz en la que se indi_ ca por un lado las afectaciones a la información, y por otro, los erro-- res que la provocarían.

Los resultados obtenidos fueron los siguientes:

El porcentaje más alto se localizó en los errores cometidos por -- los operadores del computador (inciso g), el cual fue del 15.051%, a su_ vez, la mayor frecuencia se registró en (rara vez), con un 7.526%, ésto_ se debe a que no se da capacitación al personal, o bien a distracciones_ por parte de estas personas.

El segundo porcentaje se encuentra en los computadores descompues- tos o fuera de orden con un 12.902% (inciso a), con una frecuencia de -- 8.602%, plasmadas en (rara vez), básicamente se debe a que no se propor- ciona el debido mantenimiento preventivo, algunas personas informaron -- que estos errores llegaban a acrecentarse hasta en períodos semanales y_ mensuales 2.150%, con lo cual se deduce que no efectúan este mantenimien to adecuadamente.

Los errores de perforación se encuentran con un 11.826%, del cual_ la frecuencia con que se presenta más seguido es (diario), 6.451%, consi derando bajo el porcentaje, ya que no afecta sustancialmente el funciona miento del Centro, estos errores son detectados con las pruebas de ve

rificación que son realizadas por todas las Unidades.

Como se observa en la gráfica, los errores de entrada a la terminal presentan un 10.751% y el mayor porcentaje identificado para la frecuencia se localiza en (diario), con un 5.376%, no perjudica a la información, ya que son detectados estos errores a través del diálogo hombre-máquina, el cual indica al usuario sobre las equivocaciones que éste cometa para que sea corregido en ese momento.

Las cintas o discos extraviados (inciso i), así como los daños físicos a éstos (inciso d), alcanzaron un 8.601%, la más alta reincidencia para cada uno de los casos se apunto en (rara vez), con un 6.451%, ésto resulta en el primer aspecto grave, porque la información puede ser utilizada para venderla o sobornar a la institución, en el segundo caso, - no resulta tan grave, ya que todas las Unidades aseguraron que contaban con archivos de soporte, por lo tanto, al sufrir algún daño los archi-- vos, se puede contar con los de respaldo.

En discos u otros volúmenes que no se puedan leer (inciso b), se indica un 7.526% aquí sucede como en el caso anterior, la situación no afecta grandemente al Centro, debido a que se cuentan con los archivos de respaldo.

Una vez más notamos que no se proporciona un mantenimiento adecuado al equipo de cómputo, así lo demuestra el porcentaje alcanzado en -- tarjetas mutiladas por la máquina que fue del 6.451%, aunque se preser

tó con períodos mensuales y semestrales con un 1.075% para cada uno y - rara vez con 4.301%; ésto no debería suceder si se da el servicio requerido al equipo.

Un 5.375% se asentó en los errores en la transmisión de datos por fallas del equipo, este inciso (c) se encuentra relacionado con la pregunta 13, ya que todos los Centros de Cómputo cuentan con algún código de control, el cual detectará las fallas del equipo, considerando no gravosa esta situación.

Aunque parece difícil concebir descuidos tales como volúmenes actualizados equivocadamente, éstos alcanzaron un porcentaje del 4.300%, debido a que no se lleva un control adecuado de los mismos.

El inciso (m) uso de una terminal para diversión, registró un 2.150%, aunque el porcentaje es bajo, sí puede afectar a la información cuando se haga uso de los archivos, pero si se cuenta con programas diseñados para estos caso, no ocasiona ningún problema, cabe hacer notar que este último caso es al que se refirieron las personas entrevistadas, informando que sí contaban con este tipo de programas.

El inciso que registró el mismo porcentaje del anterior, fue para inundaciones, ésto se debe a la mala ubicación del Centro, ya que éstos se encontraron localizados en la planta baja del edificio, ésto puede ocasionar un grave daño, ya que afectaría todo el equipo de cómputo

dejando a la Unidad sin procesar su información, ocasionando serios problemas a la institución.

El 1.075% se prestó para saqueo, sabotaje, mala fe del usuario y fuego, aunque en los 4 presentan una frecuencia de (rara vez), éstos aspectos resultan bastante delicados, los dos primeros se deben a que no cuentan con procedimientos adecuados para la vigilancia del Centro, el tercer caso resulta difícil su control, ya que no se puede contar con una persona que se encargue de estar vigilando a cada uno de los usuarios, sobre todo en sistemas en teleproceso; sin embargo, se lleva el control de quién afecta la información a través de su clave personal, así como de la clave de la terminal, con lo cual se puede identificar al usuario que actúa de mala fe.

En el caso de fuego, la persona a la que se entrevistó, indicó que no ocasionó daño considerable al Centro, debido a que se descubrió rápidamente, gracias a los detectores y alarmas con que cuentan, el cual fue sofocado con los extinguidores, tomando todas las precausiones necesarias tal como el apagado de la energía al cuarto.

TIPOS OE EXPOSICION OE LA SEGURIOAO

	Incapacidad para Procesar	Pérdida de un Archivo Completo	Pérdida de Registros Simples	Modificación de Registros	Lectura o copia no Autorizada
FALLAS DE HAROWARE					
a) Computador fuera de orden	X				
b) Disco u otro volumen que no se pueda leer		X			
c) Error en la transmisión de los datos por fallas del equipo			X	X	
d) Tarjetas mutiladas por la máquina			X	X	
DESCUIOOS HUMANOS					
e) Error de perforación			X	X	
f) Error de entrada del usuario a la terminal			X	X	
g) Error del operador del computador		X	X	X	
h) Volumen equivocado y actualizado		X		X	
i) Cinta o disco extraviado		X			X
j) Oaño ffsico a una cinta o disco		X	X		
DAÑO INTENCIONAL					
k) Saqueo	X	X			
L) Sabotaje	X	X			
LL) Mala fe del usuario		X	X	X	
m) Uso de una terminal para diversión		X	X	X	
n) Fraude		X	X	X	X
CATASTROFES MAYORES					
ñ) Fuego	X	X			
o) Inundación	X	X			

TIPOS DE EXPOSICION DE LA SEGURIDAD

	Incapacidad para Procesar	Pérdida de un Archivo Completo	Pérdida de Registros Simples	Modificación de Registros	Lectura o copia no Autorizada
FALLAS DE HARDWARE					
a) Computador fuera de orden	X				
b) Disco u otro volumen que no se pueda leer		X			
c) Error en la transmisión de los datos por fallas del equipo			X	X	
d) Tarjetas mutiladas por la máquina			X	X	
DESCUIDOS HUMANOS					
e) Error de perforación			X	X	
f) Error de entrada del usuario a la terminal			X	X	
g) Error del operador del computador		X	X	X	
h) Volumen equivocado y actualizado		X		X	
i) Cinta o disco extraviado		X			X
j) Daño físico a una cinta o disco		X	X		
DAÑO INTENCIONAL					
k) Saqueo	X	X			
L) Sabotaje	X	X			
LL) Mala fe del usuario		X	X	X	
m) Uso de una terminal para diversión		X	X	X	
n) Fraude		X	X	X	X
CATASTROFES MAYORES					
ñ) Fuego	X	X			
o) Inundación	X	X			

C A P I T U L O IV

CONCLUSIONES Y RECOMENDACIONES

10. CONCLUSIONES

A continuación se presenta el cuadro que sirve de base para comprobar o disprobar la hipótesis planteada, el cual se elaboró tomando - aquellos porcentajes de cada pregunta que ofrecen una mayor seguridad.

Cabe hacer notar que las preguntas 10, 12 y 18, no fueron tomadas en cuenta, ya que sirvieron de control; asimismo la pregunta 25 no_ se consideró por ser una pregunta complementaria.

Para representar los porcentajes de las preguntas 21 y 23, se tomó en cuenta el total obtenido, menos el porcentaje de aquellos incisos que especificaban que no se lleva ningún control, debido a que no se ha-

ce necesario contar con todas las alternativas enunciadas en cada pre-- gunta para alcanzar un mayor grado de seguridad.

CUADRO QUE COMPRUEBA O DISPRUEBA LA HIPOTESIS

PREGUNTA NUMERO	ALTERNATIVA DE MAYOR SEGURIDAD	PORCENTAJE
1	(a)	100.000
1a	(h)	29.411
2	SI	93.333
3	SI	93.333
4	SI	53.333
5	(c)	100.000
6	(f)	20.000
7	(c)	80.000
8	(e)	41.176
9	(d)	25.000
11	(c)	20.000
13	(d)	15.384
14	SI	66.666
14a	SI	66.666
15	(e)	18.181
16	(a)	53.571
17	SI	93.333
19	SI	93.333
20	SI	100.000
21		94.116
22	(g)	4.000
23		92.588
24	SI	100.000
	TOTAL:	1453.424 %

1453.424% ÷ 23 preguntas = 63.192%

Con este último resultado 63.192%, queda disprobada la hipótesis planteada "Sí se aplican las medidas de seguridad en los Centros de Cómputo del Sector Público Central en un 80%".

Por todo lo anterior, se concluye que las Unidades de Informática del Sector Público Central necesitan establecer sus programas de seguridad, los cuales deben ser diseñados para proteger sus instalaciones, tanto de actos catastróficos, que rara vez ocurren como fuego e inundaciones, así como de hechos relativamente menores como puede ser el daño a registros individuales, los cuales pueden ocurrir varias veces en una semana, teniendo presente cada uno de los componentes del sistema, evitando de esta forma, que se deje alguna parte desde la cual se pueda causar daño.

11. RECOMENDACIONES

En base a los resultados obtenidos en la realización de esta investigación, me permito hacer las siguientes sugerencias:

1a. Todo sistema de seguridad debe tener una serie de responsabilidades distribuidas para hacerlo más seguro. Algunas de estas responsabilidades pueden ser las siguientes:

- Los programadores de sistemas no deberán escribir programas de aplicación y viceversa.

- No se debe permitir a los usuarios el acceso a los programas de aplicación, excepto por medio del software de control de entradas/salidas, el cual deberá contener ciertas

medidas de seguridad entre las que se incluyen la identificación del usuario y las pruebas de autorización.

- No se debe permitir que un programa de aplicación accese a los archivos de datos, excepto por medio del software de -- administración de datos, el cual deberá contener medidas - de seguridad, incluyendo palabras clave y pruebas de autorización.

- Los programadores no deberán estar autorizados para operar el equipo de cómputo.

- Los operadores no deberán ser informados de las funciones_ que realizan los programas que corran.

- Las cubiertas de cintas y discos deberán estar etiquetadas con números alfanuméricos sin que indiquen su función.

- Ningún programa debe ser corrido si no está catalogado en_ la biblioteca de programas.

- Se deberá mantener un control estrecho sobre los programas nuevos que se vayan a catalogar en esta biblioteca, ya que deben estar completamente autorizados.

- Los usuarios del sistema presentarán sus programas sin especificarlos en detalle, ya que de eso se encargarán los analistas o los programadores.

- Las especificaciones de los programas deben ser aprobados por un grupo de control de la programación.

- Las especificaciones para registros o archivos de bases de datos deben ser aprobadas, tal vez por el mismo grupo que aprobó las especificaciones de datos.

- Los datos para una prueba final de un programa no deben ser generados por el programador que crea el programa, sino por un grupo establecido para ese propósito.

- Las pruebas a los programas no las debe realizar el programador que los creó sino el grupo de control de la programación quien deberá controlar estrechamente esta operación.

- Todos los programas y las modificaciones que sufran posteriormente, deberán ser catalogadas en una biblioteca de programas, incluyendo datos acerca de quién programó y quién autorizó las modificaciones.

- Los grupos de operación que manejan las corridas del sistema pueden estar separados en funciones de operación y prueba y funciones de soporte.

- Los programas de aplicación para funciones críticas no deben ser escritos por el mismo programador.

2a. Para lograr un control efectivo en la detección y corrección de errores, se necesitan los siguientes elementos:

- Un diálogo hombre-máquina diseñado apropiadamente para detectar el máximo posible de errores y que prevea una retroalimentación adecuada para los usuarios.

- Un examen y balance fuera de línea.

- Una acción humana inteligente y flexible para detectar y corregir los errores que pasaran inadvertidos.

3a. Una de las funciones importantes es el mantenimiento de los archivos, por lo cual es necesario incluir las siguientes actividades:

- Conservar las cintas en buen estado y reponerlas oportunamente antes de que su vida útil empiece a declinar.

- Verificar periódicamente que no haya fallas del equipo al momento de copiar de disco a cinta el archivo de salida al término de un proceso.

- Conservar una bóveda a prueba de fuego y agua, las cintas con el respaldo de los archivos, programas o sistemas operativos. Esta bóveda deberá estar localizada preferentemente fuera de la Unidad de Informática, ya sea en un banco o en otro edificio protegido.

- Los programas y procedimientos para la reconstrucción de archivos deberán estar totalmente desarrollados y probados antes de que el sistema sea puesto por primera vez en operación, cuando se presentan mayores y más frecuentes daños en los archivos, debido tanto a los errores de programa no detectados, como a la falta de familiaridad de los operadores con su nuevo trabajo.

B I B L I O G R A F I A

1.- James Martin, Security, Accuracy And Privacy In Computer Systems, Pretice-Hall, Inc., New Jersey, 1980.

2.- Katzan, Harry Jr., Computer Data Security, Van Nostrand Reinhold, New York, 1978

3.- Van Tarsel, Dennis, Computer Security Managment, Pretice-Hall, -- Inc. New Jersey, 1979.

4.- 42 Suggestions For Improving Security In Data Procesing Operations, I.B.M., G520-2797-0

5.- Data Security Controls And Procedures A Philosphy For D.P. Installations, I.B.M., G320-5649-00

6.- Murdick G., Robert y Ross E.Joel, Sistemas de Información Basados en Computadoras para la Administración Moderna, México, Ed. Diana, 1974.

7. Laza Cerna Humberto, Higiene y Seguridad Industrial, México, Ed.- Porrua, 1973.

8.- Blake Roland P., Seguridad Induserial, Ed. Diana, México, 1973.