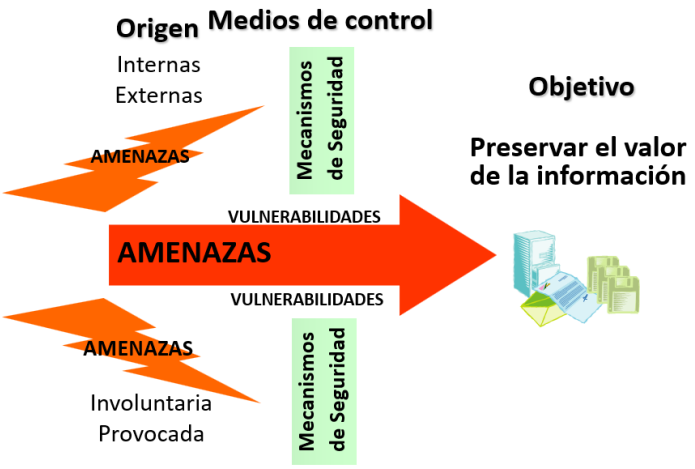
Tabla de contenidos

Conceptos de Seguridad

- “El único sistema seguro es aquel que: está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él.” - Gene Spafford - Professor of Computer Sciences and Philosophy, Purdue University
- "La combinación de espacio, tiempo y fuerza, que deben considerarse como los elementos básicos de esta teoría de la defensa, hace de ésta una cuestión complicada. Por consiguiente, no es fácil encontrar un punto fijo de partida". De la guerra, Karl Von Clausewitz.
- “El arte de la guerra nos enseña a confiar no en la posibilidad de que el enemigo no venga, sino en nuestra propia disponibilidad para recibirlo; no en la oportunidad de que no ataque, sino en el hecho de que hemos logrado que nuestra posición sea inexpugnable”. El arte de la guerra, Sun Tzu.

	In God we trust. All others, we monitor

La seguridad como estrategia



El ambiente de negocio electrónico abre nuevos riesgos en el manejo de la información de la institución, los cuales deben ser evaluados y manejados apropiadamente

Balance

RIESGOS vs NEGOCIO

Ecuación del Riesgo

RIESGO = amenazas X vulnerabilidades

- Riesgo
- Vulnerabilidad
- Exposición

¡ El riesgo nunca puede ser cero !
(Riesgo Residual)

A nivel organizacional

Proverbio…

"El empleado solo hace lo que el jefe controla"

El factor humano es PRIMORDIAL

Controles

1. Fisicos
2. De acceso

En realidad, de ingreso y egreso…

3. Seguridad de Datos
4. Comunicaciones
5. Administrativos

Seguridad por Controles Físicos

- Keys (llaves, tarjetas)
- Locks (teclado)
- Antropométricas
- Voz
- Huellas Dactilares
- Scanning del Iris

2. Controles de acceso

1. Algo que se "conoce"
   - Password
2. Algo que se "tiene"
   - Smart card or token
3. Algo que se "es"
   - Firma, voz, huellas dactilares, scanneos → Biometría

- Actualmente se combinan las 3

Biometricos

- Foto (cambia con la edad)
- Huella dactilar (modificable)
- Geometria de la mano (cambia)
- Retina
- Voz (resfrio, laringitis, etc.)
- Firma (Nunca "sale" igual)

3. Seguridad de Datos

- Confidencialidad
- Acceso (eyes only)
- Integridad

4. Comunicación

- Formas de Control
- Paridad de datos
- Disparidad de datos
- CRC
- Encriptación
- Validación

Principios de Seguridad

- Minimos privilegios
  - De acceso a los recursos
- Minima exposicion
  - Que no se vea mas que lo necesario

5. Controles Administrativos

- Estándares
- Separación de funciones
- Auditorias periódicas
  - Oportunidad para los de Ciencias Económicas, en áreas de Auditoria Interna

Controles de Aplicacion

- Entrada
- Procesos
- Salida
  - Son las distintas “validaciones”

5. Controles Administrativos

- Apropiada seleccion, capacitacion y supervision de los empleados.
- Lealtad a la empresa
- Revocacion inmediata de privilegios a empleados desvinculados o transferidos.
- Modificacion periodica de la forma de acceso.

Tipos de delitos informáticos reconocidos por Naciones Unidas

Fraudes cometidos mediante manipulación de computadoras

Manipulación de los datos de entrada

- Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de estos.

La manipulación de programas

- Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida

- Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática

- Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones informáticas.

- Como objeto
    - Cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumentos
    - Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados.

Sabotaje informático

- Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Virus

- Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos

- Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica

- Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Acceso no autorizado a servicios y sistemas informáticos

- Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Piratas informáticos o hackers

- El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con

frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Phishing:

- Este tipo de delito informático se lo conoce como “phishing”, y consiste en el envío de correos electrónicos, en los cuales el destinatario cree que el remitente se trata de una entidad reconocida y seria (usualmente bancos u organizaciones como el Consejo), en los que se solicita al usuario que por unos u otros motivos actualice o verifique sus datos de cliente a través, normalmente, de un enlace a una página que simula ser de la entidad suplantada. Una vez que el usuario remite sus datos, los estafadores pueden operar con los mismos.
- La intención de estos delincuentes cibernéticos es adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.
- El envío de un email solicitando el cambio de datos no es la forma habitual de actuar en organizaciones como nuestro Consejo, por lo que cualquier notificación por este medio que se reciba se recomienda que se verifique antes de hacer nada poniéndose en contacto con nosotros.

Reproducción no autorizada de programas informáticos de protección legal

- Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Ataques de los Virus

- Interrupcion
  - Cortar el flujo de comunicaciones
  - Cortar el acceso a dispositivos
  - Cortar la comunicacion entre equipos
  - Ocupacion de canales

Ataques de los Virus

- Intercepcion
  - Tener acceso a un mensaje
  - Leer alguna transmision
  - Acceder al trafico de un canal

Ataques de los Virus

- Espionaje
  - Aprender de algun sistema
  - Robar datos
  - Key recorders
  - Tracking de transacciones

Ataques de los Virus

- Modificaciones
  - Cambiar informacion
  - Alterar programas
  - Reordenar archivos
  - Cambiar localizacion de los datos

Ataques de los Virus

- Destruccion
  - Romper programas
  - Inutilizar equipos
  - Sobrecargar los equipos
  - Atacar hardware

Ataques de los Virus

- Integridad
  - Que existan varios valores de los datos
  - Alteracion de registros
  - Modificar los back-ups

De nuevo...

La menor cantidad de errores en el ingreso de datos se produce cuando la captura de datos es efectuada en el punto mas cercano al que registra la transacción

GIGO = Garbage In – Garbage Out

Backup

- Dado que resulta prácticamente imposible, debido a limitaciones tecnológicas y sobre todo financieras, almacenar en copias de respaldo todos los datos que posee una organización para su recuperación y disposición inmediata, es necesario clasificar los datos de acuerdo con el grado de importancia para las funciones básicas de la organización.

De este modo los datos pueden clasificarse de 3 formas:

1. ***Datos críticos***: Corresponden a los datos sin los cuales la organización no puede continuar con sus operaciones.
2. ***Datos necesarios***: Se encuentran en esta categoría todos los demás datos que son necesarios para la compañía, pero no de forma inmediata ya que las operaciones no se paralizarían sin ellos, al menos no en el corto plazo.
3. ***Datos innecesarios o fuera de respaldo***: Son los datos que en el caso de que se pierdan no hay necesidad de recrearlos.

- Una vez identificados los diferentes datos críticos se debe determinar cuánto tiempo puede seguir operando el negocio sin cada uno de ellos, y así determinar el *Tiempo de Recuperación Requerido* para cada dato. En este punto es importante evitar clasificar todos los tipos de datos como que requieren recuperación inmediata ya que en muchos casos no lo son realmente y esto lleva a un desperdicio innecesario de recursos. Esto es, cuanto mayor sea la velocidad a la que se necesiten recuperar los datos, mayor será el costo de la protección.
- La copia de seguridad en cinta es el método tradicional de almacenamiento de datos de respaldo. Mediante este sistema un dispositivo de almacenamiento en cinta es conectado a un servidor y con la ayuda de un software específico se realizan copias de respaldo de los datos del servidor a cinta con una periodicidad programada. Las cintas son cambiadas por un empleado de la compañía asignado a tal efecto y las cintas viejas son almacenadas en un depósito fuera de la compañía. Para recuperar datos, la cinta que los contiene es buscada en el depósito y llevada nuevamente a la organización donde se procede a la extracción de los archivos.
- El avance en las tecnologías de almacenamiento de datos permite hoy en día, y seguramente se establecerá como estándar en el mediano plazo, la implementación de dispositivos de almacenamiento ópticos (DVDr) que reemplazaran a la cinta debido a la gran capacidad, creciente velocidad y cada vez menor costo así también como su alta confiabilidad y duración ya que prácticamente no se deterioran con el paso del tiempo.
- *Ventajas*: Almacena datos fuera de la compañía para protegerlos contra robos y desastres dentro de la misma y provee un archivo de datos previos.
- *Desventajas*: El almacenamiento en cinta no es del todo confiable. Además, requiere intervención y monitoreo constante de personas. Por otro lado, al estar almacenadas en otro lugar, en el caso de necesitar recuperar datos en forma urgente, es decir, en el momento, la limitación de la distancia demora el proceso.
- Entre ellas se encuentran los métodos en los que se utilizan RAIDs para replicar los datos contenidos en un disco primario y almacenarlos en un disco secundario dentro de la organización copiándolos

continuamente, creando de este modo una imagen idéntica de los datos originales. De esta forma si el dispositivo de almacenamiento principal sufriera algún desperfecto, la organización podría seguir operando, utilizando los datos duplicados en los dispositivos de almacenamiento de respaldo.

- *Ventajas*: Provee una copia de los datos críticos actuales que pueden estar disponibles en forma inmediata. También reduce la principal causa de perdida de datos, las fallas del hardware.
- *Desventajas*: Se limita a proteger contra fallas del hardware. Si un dato original es borrado o corrompido, el daño se duplicará en la copia de respaldo y no se podrá revertir.

Replicación Off-Site

- Este método utiliza software de replicación y una conexión de red para copiar los datos de un servidor original a uno ubicado fuera de la organización donde es guardado como copia de respaldo. Los datos se transmiten vía Internet o una conexión de red privada entre los dos lugares.
- *Ventajas*: Provee una copia de los datos críticos actuales los cuales se almacenan fuera de la organización, protegiéndolos de daños físicos. Los datos están disponibles en forma inmediata. También reduce la principal causa de perdida de datos, las fallas del hardware.
- *Desventajas*: El costo del hardware y el software puede ser demasiado elevado y como en la redundancia de datos si un dato original es borrado o corrompido, el daño se duplicará en la copia de respaldo y no se podrá revertir.

Servicio de Administración de Backup Online o en la nube

- Esta solución combina aspectos del backup en cinta y la replicación off-site brindando una solución tercerizada. En primer lugar, se replican los datos a través de Internet mediante una conexión de banda ancha, en un servidor que está ubicado fuera de la organización y que pertenece a quien brinda el servicio. Los datos del servidor de respaldo son archivados en cinta en intervalos regulares y son almacenados en lugares seguros. La recuperación de datos puede realizarse en forma inmediata a través de la misma conexión a internet.
- *Ventajas*: Permite el acceso tanto a datos recientemente copiados como a datos históricos. Los datos son almacenados off-site, pero pueden ser recuperados en minutos. Los backups se realizan en forma automática lo cual no permite que se produzcan errores por la intervención de humanos.
- *Desventajas*: Requiere una conexión con un ancho de banda suficiente. Para más de 20 GB de datos es necesaria una conexión T1, para las menores alcanza con una DSL. Si se necesita un ancho de banda superior para usar el servicio, el costo total puede ser muy elevado.

Clasificaciones de Backup

De acuerdo con cómo se realice el método de backup pueden diferenciarse varias clasificaciones las cuales no son excluyentes entre sí, sino más bien complementarias.

Según cantidad relativa de datos

- Backup completo, diferencial o incremental.
- Se pueden combinar de varias formas. Siempre debería guardarse una copia de seguridad completo off-site.
- En una copia de seguridad completo se almacenan la totalidad de los datos necesarios de una organización.
- En una copia de seguridad diferencial se guardan todos los datos que fueron modificados desde que se realizó el último backup completo o incremental.
- En una copia de seguridad incremental se guardan todos los datos que fueron modificados desde que se realizó el ultimo backup haya sido este completo, diferencial o incluso incremental. La ventaja del backup incremental es que es más rápido que los demás, pero en el momento de la recuperación de datos será más lento el proceso.

Según la periodicidad con que se realiza

- Puede ser semanal, diaria, por hora, etc.
- La periodicidad con que se realicen las copias de respaldo estará dada por las necesidades específicas de cada compañía. Tal vez sea innecesario para una compañía pequeña realizar backups completos todos los días. Podría, en cambio, realizar backups incrementales diarios y completos en forma semanal. Sin embargo, grandes compañías que manejen grandes volúmenes de datos en forma diaria tal vez necesiten realizar backups por hora, ya que no pueden permitirse perder los datos recolectados durante las anteriores 23 horas si realizaran backups diarios.

Según en qué tipo de equipo se realice

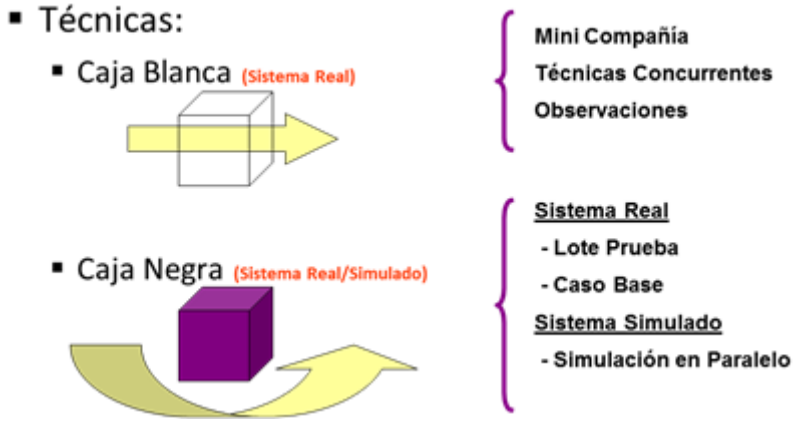
- Las posibilidades son: servidor o estación de trabajo.
- Mientras que una estación de trabajo se maneja por sí misma, en un servidor influyen la actividad de los dispositivos instalados y la red. La diferencia entre ambos está dada en la en los requerimientos de performance de los componentes de backup.

Según desde donde se realice.

- Puede ser backup local o remoto.
- Concierne solamente a lo relacionado con los servidores. Para hacer una copia de seguridad remoto en una estación de trabajo es necesario que esta se conecte con un servidor. La cuestión es si se realiza la copia de seguridad dentro o fuera del establecimiento. Independientemente de donde se realice el proceso de backup, las copias de respaldo deben almacenarse off-site.


Gobierno Corporativo
Gobierno de TI
Seguridad
Auditoria Financiera
Auditoria de los Sistemas de Información
Evaluación del rendimiento de sistemas
CAAT,s.
Auditoria Operativa

Auditoria: Pruebas de cumplimiento de controles – Técnicas aplicables



▪ WALKTHROUGH ▪ Seguir a través del sistema ▪ Se ve el detalle en cada paso ▪ CAJA BLANCA	▪ POR FUERA DEL SISTEMA ▪ SE VEN CHECK-POINTS ▪ CAJA NEGRA ▪ Solo se conocen cosas específicas ▪ Entradas ▪ Salidas ▪ Algunos procesos (resultado de ellos)

¿Cómo se audita un sistema?

- Pruebas
  - De cumplimiento de Controles
    - Determinar si el sistema se comporta como se espera que lo haga
    - Gestión del ente
- Sustantivas
    - Obtener evidencias que permitan opinar sobre:
      - Integridad
      - razonabilidad y
      - validez
      - de lo producido por el sistema de Información

El riesgo de auditoria

- Riesgo inherente:
  - un error puede ser material si se combina con otros errores encontrados en la auditoria y

no existen controles compensatorios.
    - Es el riesgo propio del negocio, riesgo de que haya un error sin considerar la efectividad del control interno. Riesgo de ocurrencia de un error
- Riesgo de control:
    - el sistema de control interno no puede detectar o evitar un error material en forma oportuna. Riesgo de ocurrencia de un error
- Riesgo de detección:
    - el auditor concluye que no existen errores materiales y hay. Riesgo de no detectar un error

Clasificación de controles claves

Control: se define como Control a cualquier medida de protección orientada a asegurar que se preserve la Confidencialidad, Disponibilidad e Integridad de los Activos de Información. Algunos ejemplos de controles son:

- Segregación de funciones.
- Respaldo de información.
- Sistemas de detección y extinción de incendio.
- Chequeo de acceso a lugar restringido.
- Resguardo de material peligroso (identificación por etiquetado, lugar de almacenamiento)

Controles Preventivos:

- Su propósito es impedir eventos que afecten la Confidencialidad, Integridad y Disponibilidad de los Activos de Información.
- Evitan o reducen que se produzcan errores, omisiones, actos maliciosos. Guían para que las cosas se hagan como se deben. Generalmente son pasivos es decir que no toman una acción física.
- Ejemplos:
    - Definición de responsabilidades
    - Confiabilidad en el personal
    - Entrenamiento
    - Capacitación o percepción de la seguridad
    - Personal competente
    - Separación de tareas
    - Rotación de tareas
    - Estandarización
    - Autorización
    - Redundancia
    - Diseño de formularios
    - Utilización de UserId o tarjetas

- Uso de contraseña
- Cambio periódico de contraseña
- Terminales que se desactivan luego de 3 intentos no autorizados
- Formularios pre numerados
- Máscaras de entrada
- Cancelación de documentos
- Archivo de documentos fuentes
- Políticas, Estándares y Procedimientos documentados
- Software de control de acceso
- Firewalls
- Terminales que se desactivan luego de 3 intentos no autorizados
- Utilización de tarjetas de identificación de empleados

Controles detectivos:

Detectan que se han producido errores, omisiones, actos maliciosos e informan su aparición. Monitorean el proceso, registran los problemas y sus causas, determinan si el control preventivo funciona.

Actúan a posteriori que se produce la transacción.

Está diseñado para detectar intentos de penetrar las barreras de seguridad implementadas, o el uso inapropiado de los activos de información

- Ejemplos:
  - Registro histórico (log) de violaciones de acceso (grabación y examen del log). Es un control detectivo, pero no es un control de aplicación detectivo.
  - Las pistas de auditoría si bien son controles detectives no es el propósito primario de los controles detectivo
  - Remito de movimientos
  - Numeración de lotes
  - Totales de control
  - Cuenta de transacciones
  - Control de secuencia
  - Digito verificador
  - Registro de fecha y hora
  - Control de validez
  - Listado de control
  - Reconciliación
  - Archivo de pendiente
  - Totales de pendientes
  - Controles cruzados
  - Rotulación de cintas y discos
  - Verificación de autorizaciones

- Capacitación o percepción de la seguridad (también puede ser detectivo porque permite identificar posibles violaciones)
- Auditorías
- Monitoreo del uso de recursos
- Revisión de registro de eventos o incidentes.
- Sistemas de detección de intrusos (IDS)

Controles correctivos:

Corrigen errores, omisiones o actos maliciosos que se hayan detectado por ej. Ante el ingreso de una fecha errónea el sistema la corrige colocando la fecha del sistema. Reprocesan luego que fue corregido a través de estos o aún más severos controles, registran las acciones tomadas y cuestan más que los otros

- Listado de discrepancias
- Pistas de auditoría (se tienen en cuenta una vez que ha ocurrido el problema)
- Estadística de origen de errores
- Corrección automática de errores
- Respaldo operativo
- Recuperación
- El plan de recuperación de desastres documentado

Control Recuperatorio

está orientado a restaurar rápidamente los servicios y corregir el efecto de los incidentes de seguridad, así como facilitar su investigación.

- Respaldo de datos
- Soporte 7 x 24
- Planes de contingencia
- Plan de continuidad del Negocio

El mejor control es el que evita problemas (controles preventivos), luego le siguen los que identifican un problema ya que permiten tomar medidas de investigación y corrección (controles detectivos) y por último los controles para corregir un problema (controles correctivos o de recuperabilidad)

Pruebas Sustantivas

- Obtener evidencia Física, Documental y Verbal de los elementos auditados
- Criterios de comparación, confirmación y razonabilidad
- Utilizando programas que ayuden a la tarea cuando sea posible, tales como Software Específico: ACL, Cognos, Clementine
- Pistas de Auditoria (si fuesen inalterables) de las BD de los sistemas en uso
- Las pruebas de cumplimiento y sustantivas son complementarias entre sí

- A menor confianza por parte del auditor en el control interno, mayor será cantidad y calidad de pruebas sustantivas que deberá desarrollar
- A mayor riesgo en el ente auditado, mayor alcance y naturaleza de las pruebas sustantivas a realizar

Ejemplo de auditoría de sistemas en un Sistema de Liquidación de haberes: preguntas a realizar (se)

- Pruebas de Cumplimiento
  - ¿Quién liquida los haberes es distinto de...
  - ¿Quién los autoriza...?
  - ¿Quién efectúa las acreditaciones de sueldos...?
  - ¿Quién efectúa el pago de cargas sociales...?
  - ¿Quién autoriza los aumentos de sueldo...?
  - ¿Quién efectúa el cálculo de las comisiones de venta...?
  - ¿Qué periodicidad tienen estos cambios?
  - ¿Hay procedimientos establecidos en cuanto a los límites de firma para pagos y gastos? ¿Están actualizados?
  - ¿Quedan pistas de auditoría de los movimientos efectuados?
  - ¿Se efectúan cálculos manuales que se ingresen en forma directa a la liquidación?
  - ¿Hay una política establecida para el pago de horas extra y premios?
  - ¿Quién controla el presentismo/ausentismo y por qué método?
  - ¿El sistema de Liq. Haberes recibe y emite información por medio de interfaces?
  - Son interfaces de “texto”
  - ¿Se realizan provisiones en función a montos determinados por el sistema?
  - ¿En forma manual o automática?
  - ¿Son realizadas por personas distintas?
  - ¿Existe una línea de reemplazos con motivos de licencias vacacionales del personal que liquida los haberes?
  - Al utilizar el sistema ¿el usuario debe identificarse con usuario/contraseña?
  - ¿Qué mecanismo de seguridad de contraseña hay en funcionamiento?
  - ¿Expira la sesión de trabajo de un usuario luego de un determinado tiempo de inactividad?
  - ¿Existe un procedimiento para dar de baja en el acceso a los sistemas al personal desvinculado?

- Pruebas Sustantivas
  - Buscar legajos y cajas ahorro duplicados
  - Comparar retenciones practicadas y su ingreso
  - Conceptos inusuales de pago y descuento
  - Horas de entrada/salida de reloj vs. horas extra
  - Revisar la autorización de las horas extra
  - Revisar el pago de haberes por trabajos en días feriados

  - Control de días por examen y enfermedad
  - Recalcular importes determinados
  - Determinar provisiones
  - Determinar comisiones pendientes de exvendedores

- La fortaleza de las pruebas de cumplimiento influenciará la naturaleza y alcance de las pruebas sustantivas
- Hoy en día, es “económico” realizar pruebas de “caja blanca” aún para auditores externos
- Paulatinamente, “cae” la necesidad de efectuar “muestras”, debido a SW de datamining
- Las normas técnicas de auditoría NO varían por el uso de herramientas tecnológicas – RT 37
- La normativa profesional, expone QUE debe hacerse, pero no COMO.