

**Universidad Católica Boliviana “San Pablo”
Facultad de Ciencias Exactas e Ingeniería
Ingeniería de Sistemas**



“RESUMEN CAPITULO 6 : EVALUACION DE SEGURIDAD”

Materia: Auditoria de Sistemas

Paralelo: 1

Alumnos:

- Daniel Andres Aramayo Bejarano
- Johan Federico Arispe Rodriguez
- Sergio Daniel Ballesteros Ferrel
- Freddy Salvador Valda Sanchez
- Andrés Mauricio Prudencio Robinson
- Sergio Willy Ossio Marín

Catedrático: PhD. Indira Guzmán

CAPITULO 6: EVALUACION DE LA SEGURIDAD

1. SEGURIDAD LOGICA Y CONFIDENCIALIDAD

La información puede ser de suma importancia y las computadoras son el instrumento que estructuran grandes cantidades de información. La información puede ser confidencial y está expuesta a ser divulgada o mal utilizada. Además cuando esta información no es disponible en determinado momento puede generar pérdidas en una empresa.

La criminología dio un giro y abrió un nuevo mundo de crímenes informáticos, donde las computadoras son el medio para estos fines. Los más comunes fueron realizados a bancos, donde se realizan transferencias y grandes robos, además de esto se puede cambiar y manipular la información.

Los virus son otro problema de seguridad, son pequeñas subrutinas que tienen malas intenciones y pueden eliminar información, robarla, modificarla, provocar congestiones, entre otros.

Existe un incremento en los crímenes por computadora debido al aumento del número de personas que estudian computación, la gran cantidad de empleados que tienen accesos y el incremento de las aplicaciones existentes.

Un sistema integral de seguridad debe tener al menos:

- Política de Seguridad
- Elementos Administrativos
- Organización de responsabilidades
- Seguridad física
- Elementos técnicos y procedimientos
- Sistemas de seguridad

En algunos casos cuando un servicio se interrumpe puede significar grandes pérdidas, en otros no tanto, por lo cual se debe determinar el costo/beneficio de los sistemas de seguridad frente a la pérdida de información. El nivel de riesgo debe establecerse para todas las aplicaciones además de verificar cuales serían las consecuencias en caso que no funcione o se detenga. Un ejemplo de alto riesgo son los bancos, reservaciones o casas de bolsa donde se deben tener sistemas funcionando en paralelo, sistemas de energía no interrumpible.

Para la auditoría se debe elaborar una lista con todos los elementos nombrados previamente, determinar el nivel de riesgo y las medidas preventivas a tomar.

Sistema o información	Nivel de riesgo	Medidas preventivas
Transacciones monetarias	Alto	Energía no interrumpible, sistema paralelo, backups diarios
Videoclub, clientes	Bajo	Backup mensual
Información confidencial del mercado	Alto	Restricción en el acceso, respaldos
Nomina	Medio	Respaldo

2. SEGURIDAD EN EL PERSONAL

Un centro de cómputo depende de la integridad, estabilidad y lealtad del personal.

Se deben considerar:

- Evitar la dependencia de ciertas personas
- Política de reemplazo
- Políticas de rotación de personal
- Motivación del personal

3. SEGURIDAD FISICA

Básicamente trata de establecer políticas, procedimientos y prácticas para evitar interrupciones del servicio, información debido a catástrofes como incendios, inundaciones, tsunamis, disturbios, huelgas, sabotajes, etc.

Algunas consideraciones

- Los equipos centrales no deben ser visibles a todo el público
- El material del centro de cómputo no debe ser inflamable
- Evitar lugares sumamente calurosos
- Ductos de aire acondicionado limpios
- Fuente de energía no interrumpible en algunos casos
- Extintores, su acceso, peso, estado
- Verificar que el personal sepa utilizar los extintores
- Salidas de emergencia

CUESTIONARIO

1. ¿Se han adoptado medidas de seguridad en la dirección de informática?
SI () NO ()
 2. ¿Existe una persona responsable de la seguridad?
SI () NO ()
 3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
SI () NO ()
 4. ¿Existe personal de vigilancia en la institución?
SI () NO ()

 5. ¿La vigilancia se contrata:
Directamente? ()
Por medio de empresas que venden ese servicio? ()
 6. ¿Existe una clara definición de funciones entre los puestos clave?
SI () NO ()
 7. ¿Se investiga a los vigilantes cuando son contratados directamente
SI () NO ()
 8. ¿Se controla el trabajo fuera de horario?
SI () NO ()
 9. ¿Se registran las acciones de los operadores para evitar que realicen alguna que pueda dañar el sistema?
SI () NO ()
 10. ¿Existe vigilancia en el cuarto de máquinas las 24 horas?
SI () NO ()
 11. ¿A la entrada del cuarto de máquinas existe
Vigilante? ()
Recepcionista? ()
Tarjeta de control de acceso? ()
Nadie? ()
 12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?
SI () NO ()
 13. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?
Sí () NO ()
 14. ¿El edificio donde se encuentra la computadora está situado a salvo de:
Inundación? ()
Terremoto? ()
Fuego? ()
Sabotaje? ()
 15. ¿El centro de cómputo da al exterior?
SÍ () NO ()
 16. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que fue construido y equipo (muebles, sillas, etc.) dentro del centro.
-
-
-

17. ¿Tiene el cuarto de máquinas una instalación de escaparate y, si es así, pueden ser rotos los vidrios con facilidad?

SI () NO ()

18. ¿Existe control en el acceso a este cuarto

Por identificación personal? ()

Por tarjeta magnética? ()

Por claves verbales? ()

Otras? ()

19. ¿Son controladas las visitas y demostraciones en el centro de cómputo?

SI () NO ()

¿Cómo son controladas?

20. ¿Se registra el acceso al cuarto de personas ajenas a la dirección de informática?

SI () NO ()

21. ¿Se vigilan la moral y el comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?

SI () NO ()

22. ¿Existe alarma para

Detectar fuego (calor o humo) en forma automática? ()

Avisar en forma manual la presencia del fuego? ()

Detectar una fuga de agua? ()

Detectar magnetos? ()

No existe . ()

23. ¿Estás alarmas están

En el cuarto de máquinas? ()

En la cintoteca y discoteca? ()

24. ¿Existe alarma para detectar condiciones anormales del ambiente?

En el cuarto de máquinas ()

En la cintoteca y discoteca ()

En otros lados ()

¿Cuáles?

25. ¿La alarma es perfectamente audible?

SI () NO ()

26. ¿Esta alarma también está conectada

Al puesto de guardias? ()

A la estación de bomberos? ()

A ningún otro lado? ()

Otro () _____

27. ¿Existen extintores de fuego

Manuales? ()

Automáticos?

No existen

28. ¿Se ha adiestrado el personal en el manejo de los extintores

SI NO

29. ¿Los extintores, manuales o automáticos, funcionan a base de

TIPO SÍ NO

Agua?

Gas?

Otros

30. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores

SI NO

Nota: verifique el número de extintores y su estado.

Nro: _____ Estado: _____

31. Si es que existen extintores automáticos, ¿son activados por los detectores automáticos de fuego?

SI NO

32. Si los extintores automáticos son a base de agua, ¿se han tomado medidas para evitar que el agua cause más daño que el fuego?

SI NO

33. Si los extintores automáticos son a base de gas, ¿se han tomado medidas para evitar que el gas cause más daño que el fuego?

SÍ NO

34. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos, para que el personal Corte la acción de los extintores por tratarse de falsas alarmas? SÍ NO

Pueda cortar la energía eléctrica? SI NO

Pueda abandonar el local sin peligro de intoxicación? SÍ NO

Es inmediata su acción? SI NO

35. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

SÍ NO

36. ¿Saben qué hacer los operadores del cuarto de máquinas en caso de que ocurra una emergencia ocasionada por fuego?

SI NO

37. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?

SI NO

38. ¿Existe salida de emergencia?

SI NO

39. ¿Esta puerta sólo es posible abrirla:

Desde el interior?

Desde el exterior?

Ambos lados

40. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?

SÍ NO

41. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?

SI NO

42. ¿Se han tomado medidas para minimizar la posibilidad de fuego:

Evitando artículos inflamables en el cuarto de máquinas?

Prohibiendo fumar a los operadores en el interior?

Vigilando y manteniendo el sistema eléctrico?

No se ha previsto

43. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del cuarto de máquinas para evitar daños al equipo?

SÍ NO

44. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso?

SI () NO ()

45. ¿Se controla el acceso y préstamo en la:

Discoteca? ()

Cintoteca? ()

Programoteca? ()

46. Explique la forma como se ha clasificado la información vital, esencial, no esencial, etc.

47. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?

SI () NO ()

48. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad, etc.) que garantice su integridad en caso de incendio, inundación, terremoto, etc.

49. ¿Se tienen establecidos procedimientos de actualización a estas copias?

SI () NO ()

50. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información.

0 1 2 3

51. ¿Existe departamento de auditoría interna en la institución?

SI () NO ()

52. ¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?

Sí () NO ()

53. ¿Qué tipos de controles ha propuesto?

54. ¿Se cumplen?

SI () NO ()

55. ¿Se auditan los sistemas en operación?

SI () NO ()

56. ¿Con qué frecuencia?

Cada seis meses ()

Cada año ()

- Otra (especifique) () _____
57. ¿Cuando se efectúan modificaciones a los programas, a iniciativa de quién es?
Usuario ()
Director de informática ()
Jefe de análisis y programación ()
Programador ()
Otras (especifique) () _____
58. ¿La solicitud de modificaciones a los programas se hacen en forma:
Oral? ()
Escrita? ()
En caso de ser escrita solicite formatos.
59. Una vez efectuadas las modificaciones se presentan las pruebas a los interesados?
Sí () NO ()
60. ¿Existe control estricto en las modificaciones?
Sí () NO ()
61. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?
Sí () NO ()
62. Si se tienen terminales conectadas, ¿se han establecido procedimientos de operación?
Sí () NO ()
63. Se verifica identificación:
De la terminal ()
Del usuario ()
No se pide identificación ()
64. ¿Se ha establecido qué información puede ser accesada y por qué persona?
Sí () NO ()
65. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?
Sí () NO ()
66. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
Sí () NO ()
67. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones? ¿Cuáles son?
() Recepción de documentos
() Información confidencial
() Captación de documentos
() Cómputo electrónico
() Programas
() Discotecas y cintotecas
() Documentos de salida
() Archivos magnéticos
() Operación del equipo de computación
() En cuanto al acceso de personal
() Identificación del personal
() Policía
() Seguros contra robo e incendio
() Cajas de seguridad
() Otras (especifique)

4. SEGUROS

Los seguros son un aspecto muy importante en la seguridad, pero lamentablemente no se toman en cuenta a menudo. El desconocimiento sobre tecnología de los vendedores de pólizas y el desconocimiento sobre los seguros más apropiados del personal TI hacen que sea más complicado asignar un seguro adecuado al equipo y los ambientes en los que estos residen.

Uno de los retos al momento de pensar en el seguro mas adecuado, es el costo. Ya que los tipos de riesgos pueden ser desde desastres naturales hasta hechos por negligencia, es muy difícil encontrar una póliza que cubra todo. Este hecho obliga a pensar en 2 o mas pólizas por equipo, elevando el costo de manera considerable.

5. SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO

Para evitar el deterioro de los sistemas, se debe tomar en cuenta los siguientes aspectos:

1. Accesos físicos y lógicos a la información.
2. Encriptación de datos
3. Monitoreo, supervisión y políticas de auditoria
4. Registros y logs.
5. Identificar niveles de seguridad a los diferentes equipos y datos.

Seguridad al restaurar el equipo

El riesgo del daño y pérdida de la información es real, por lo tanto se debe tener políticas claras a la hora de reparar o reanudar algún sistema o aplicación. Como elemento preventivo, se debe incluir la rutina de resguardo de la información por medio de copias de seguridad o backups.

También se deberá considerar la reconfiguración de los sistemas, evitando que el daño genere grandes consecuencias en los usuarios.

Para una correcta restauración de sistemas, deberíamos preguntarnos las siguientes cuestionantes:

- Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo.
- Enunciar los procedimientos mencionados en el inciso anterior.
- Cuentan los operadores con alguna documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones

6. PROCEDIMIENTOS DE RESPALDO EN CASO DE DESASTRE

Es importante que la dirección TI establezca un plan de emergencia. Esto es tan importante como la creación de manuales de uso. Un plan de emergencia busca cubrir los procedimientos de restauración, reconfiguración e instalación después de que algo suceda.

Al momento de crear plan de emergencia, se debe considerar los desastres tales como: completa destrucción, destrucción parcial, mal funcionamiento, pérdida de información, pérdida de personal clave, huelgas laborales.

Cuando el plan se debe ejecutar, se tiene que seguir un protocolo establecido con anterioridad. Este protocolo involucra informar a los responsables, cuantificar el daño, determinar el estado de los procesos, establecer la estrategia para llevar a cabo las operaciones de emergencia.

Lo más importante es identificar el número y tipo de componentes esenciales que puedan ser críticos en caso de emergencia o de desastre: Equipo principal, unidades de disco, unidades de cinta, unidades de almacenamiento, equipo periférico, unidades de comunicación, sistemas operativos, terminales, equipo adicional.

7. CONDICIONES, PROCEDIMIENTOS Y CONTROLES PARA OTORGAR SOPORTE A OTRAS INSTITUCIONES

Una medida de prevención y mitigación del riesgo, es establecer arreglos con otros centros para utilizar su equipo en caso de fallas mayores o en caso de desastre, como fuego, inundaciones, explosiones, etc. a fin de evitar interrupciones de los servicios de procesamiento por un largo periodo. Estos arreglos son convenientes si se llevan a cabo de una manera formal y con seriedad de compromiso.