ANEXO B

ANALISIS DE CUESTIONARIOS Y ENTREVISTAS REALIZADAS DURANTE LA INVESTIGACIÓN DE CAMPO

Con el fin de establecer las condiciones actuales de la Universidad, relacionadas con la temática del presente trabajo, se desarrollaron una serie de formularios bajo la metodología de cuestionario, preparados de acuerdo al área o personal de la Universidad involucrados, seleccionando a los entrevistados según su cargo y especialización. Se trabajo con siete formularios, los cuales fueron organizados de la siguiente manera:

- Cuestionario F1 (Diagnóstico al área gerencial): Formulario desarrollado para diagnosticar el área gerencial de la Universidad, conocer cómo las autoridades están involucradas en el tema de seguridad informática.

- Cuestionario F2 (Diagnóstico a la infraestructura tecnológica de la Universidad): Formulario desarrollado para conocer la infraestructura tecnológica actual de la Universidad, equipo de cómputo, comunicaciones, software de seguridad, etc.

- Cuestionario F3 (Diagnóstico histórico a la seguridad de los Sistema de información): Formulario elaborado para investigar sobre datos históricos relacionados con la seguridad informática de la Universidad tales como: Antecedentes de ataques, vulnerabilidades identificadas, procesos de control aplicados, etc.

- Cuestionario F4 (Diagnóstico a los bancos de información): Formulario desarrollado para diagnosticar como se administra la información almacenada en las bases de datos, funcionamiento de sistemas internos, seguridad a los bancos de información.

- Cuestionario F5 (Diagnóstico a la seguridad física y lógica): Formulario elaborado para diagnosticar los controles aplicados a nivel de seguridad física, accesos, medios físicos de protección, y además como se salvaguardan los activos a nivel de seguridad lógica, bases de datos, transacciones electrónicas, ingresos a los sistemas.
- Cuestionario F6 (Diagnóstico a la factibilidad operacional del proyecto): Formulario desarrollado para verificar la factibilidad operacional del proyecto y sustentar la viabilidad del mismo.

- Test (prueba) de seguridad: Este formulario se obtuvo de un sitio de Internet, el cual permite evaluar en línea el estado actual de los sistemas informáticos de empresas conectadas a Internet. Este test fue completado por las jefaturas de las dos unidades involucradas, luego los datos obtenidos se ingresaron en este sitio web para que evaluará la situación actual de la Institución. La dirección de este sitio es: http://ceds.nauta.es/Catal/Products/Test2.htm

El formato y contenido de cada formulario se encuentra en el anexo A.

Se utilizaron dos tipos de análisis:

- Para los formularios F1, F2, F3, F4, F5, Test de seguridad se utilizo un análisis similar a un estudio de control interno realizado por auditorías tradicionales, interpretando las respuestas obtenidas para luego elaborar un diagnostico.

- Para el formulario F6 se realizo un análisis tipo encuesta, tabulando los resultados, graficando a través de una hoja de cálculo y presentando su análisis correspondiente, esto debido a que se desarrollo para conocer el punto de vista del personal técnico de la Universidad con respecto a la elaboración de la solución propuesta.

A continuación se presenta los resultados obtenidos durante las entrevistas.

CUESTIONARIO F1 (DIAGNÓSTICO GERENCIAL)

Objetivo General: Conocer el interés y apoyo que las autoridades de la Universidad le dan al tema de seguridad de los sistemas de información.

1. ¿La Universidad desarrolla Auditorías Informáticas?

- Objetivo:
  Conocer si actualmente la Universidad cuenta con controles de Auditoría en el área de Informática.

- Respuesta:
  Si realiza Auditorías Informáticas y se llevan a cabo cada 3 meses.

- Análisis:
  De acuerdo a la fuente de la Universidad, se dice que se desarrollan auditorías informáticas cada tres meses; esta información fue verificada y se determino que se realizan únicamente auditorías a nivel financiero y auditorías operacionales por el tema de la certificación ISO 9000 y que no cuentan con un departamento de auditoría interna de planta en la Institución.

2. ¿Cuentan actualmente con una política de seguridad informática?

- Objetivo:
  Conocer si existe un documento que especifique las reglas y acciones a seguir para salvaguardar los activos informáticos de la Universidad.

- Respuesta:
  No existe actualmente, esta en desarrollo.

- Análisis:

Se determino que no cuentan con una política de seguridad informática, se menciono que esta en desarrollo; pero no se tiene fecha de cuando estaría lista.

3. ¿La Universidad destina un presupuesto para los sistemas de seguridad informática?

- Objetivo:
  Conocer si la Universidad participa económicamente en los esfuerzos por mejorar la calidad en la seguridad informática.

- Respuesta:
  Si existe.

- Análisis:
  De acuerdo a esta respuesta, la Universidad destina presupuesto anualmente al área de seguridad informática; no se conoce el monto que se destina y como se administra.

4. ¿Cuentan con contratos de seguros para proteger sus activos físicos o lógicos?

- Objetivo:
  Saber si existen pólizas de seguro que respalden los equipos contra desastres

- Respuesta:
  No tienen seguros

- Análisis:
  Se determina a través de este resultado que no cuentan con ninguna protección financiera en caso de desastres naturales, perdida de información o cualquier otro tipo de incidente que ponga en riesgo la salvaguarda de los sistemas de información.

5. ¿Existen programas de capacitación para el personal?

- Objetivo:

Verificar la aplicación de programas de capacitación para el personal

- Respuesta:
  Si se realiza

- Análisis:
  Según este resultado se están llevando a cabo capacitaciones para el personal técnico a nivel de seguridad informática, no se conoce el nivel de especialización de estas capacitaciones, ni quien o que institución las imparte.

6. ¿Están claramente definidos los roles, funciones y puestos del personal de la Dirección de Informática?

- Objetivo:
  Conocer si el personal conoce claramente sus funciones y responsabilidades dentro de la Institución

- Respuesta:
  Si existe.

- Análisis:
  De acuerdo a las fuentes entrevistas, se dice que todo el personal esta claro con sus funciones; pero no fue posible por falta de autorización obtener una copia de algún manual de puestos para verificar esta información.

7. ¿El área tecnológica es parte del plan estratégico de la Universidad?

- Objetivo:
  Saber si la Universidad cree en la tecnología como medio de crecimiento e innovación.

- Respuesta:
  Si lo consideran.

- Análisis:

  Se conoció que parte del plan estratégico de la Universidad es la tecnología.

8. ¿Quienes participan de planes de Seguridad Informática?

- Objetivo:
  Conocer quienes están involucrados de los planes de seguridad informática en la Universidad

- Respuesta:
  Dirección y jefes.

- Análisis:
  Se verifico que no se toma en cuenta al personal técnico en la gestión de seguridad de los sistemas de información. Las decisiones son tomadas por la dirección y jefatura de la unidad tecnológica y administrativa

9. ¿Cuales son los problemas que más afectan la Seguridad informática en la Universidad?

- Objetivo:
  Saber donde se centran los problemas de seguridad

- Respuesta:
  Virus y Spam

- Análisis:
  Se determinó según las fuentes entrevistadas, que los dos problemas que mas aquejan a la seguridad informática actualmente son: Los virus y Correos no deseados (Spam).

10. ¿Cuando fue aplicada la ultima medida de Seguridad Informática (SI) en la Universidad?

- Objetivo:
  Verificar la antigüedad de la última medida de seguridad aplicada

- Respuesta:
  Hace menos de un año, con la adquisición del antivirus E-Trust.

- Análisis:
  De acuerdo a esta información, la ultima acción realizada en beneficio de la seguridad de los sistemas de información, fue hace un año aproximadamente y fue específicamente con la compra de una herramienta de software de Antivirus.

11. ¿De acuerdo a su criterio, como observa el entorno de Seguridad Informática actualmente?

- Objetivo:
  Conocer como la dirección observa la gestión de seguridad informática actual

- Respuesta:
  Necesita mejorar
- Análisis:
  De acuerdo al personal entrevistado, todos consideran que la seguridad informática aun es débil y necesita mejorar.

12. ¿Donde considera necesario aplicar mayor esfuerzo para mejorar la Seguridad Informática?

- Objetivo:
  Identificar el sector donde hay que apoyar los esfuerzos de seguridad informática

- Respuesta:
  Hay dos sectores: Redes/comunicaciones y Capacitación del personal

- Análisis:

  Las fuentes determinaron que los dos sectores que más ayudaría a mejorar la seguridad informática actual son: Redes/Comunicaciones y Capacitación del personal.

13. ¿Existe interés en una certificación en Seguridad Informática a futuro?

- Objetivo:

  Conocer si existe interés por parte de la Universidad en someterse a futuro a una certificación de seguridad informática.

- Respuesta:

  Si hay interés

- Análisis:

  De acuerdo a la información obtenida, se determinó que existe interés a futuro para la aplicación de una certificación en el área de seguridad informática.

CUESTIONARIO F2 (DIAGNÓSTICO A LA INFRAESTRUCTURA TECNOLOGICA)

Objetivo general: Conocer la infraestructura de los Sistemas de Seguridad Informática de la Dirección de Tecnología y Comunicaciones (DTC) y Administración Académica.

14. ¿Como se encuentra estructurada la red local actualmente?

- Objetivo:

  Conocer los equipos de red que componen la red local de la Universidad.

- Respuesta:
  - 250 Estaciones de trabajo
  - 14 Servidores para las diferentes bases de datos y aplicaciones.

- 15 Switches, puertos 10/100 y switches de Fibra
- 1 Router
- 1 Impresor de red

- Análisis:
  Esta es la infraestructura actual de la Universidad, la cual se encarga de dar los servicios de redes y comunicaciones a todo el campus.

15. ¿Existen Subredes?

- Objetivo:
  Conocer la infraestructura de redes y analizar si realmente se adecua a los dispositivos que poseen.

- Respuesta:
  Existen 10 Subredes.

- Análisis:
  Según la persona entrevistada existen 10 Subredes, su distribución es por edificios, estas subredes se conectan por medio de fibra óptica al nodo central de UFG.

16. ¿Para el servicio de Internet se subcontrata a un proveedor de ISP (Proveedor de servicios de Internet)?

- Objetivo:
  Saber si la universidad es dueño de su servicio de Internet o subcontrata un ISP para que le pueda brindar la conexión a Internet.

- Respuesta:
  Contrata un ISP local.

- Análisis:

  De acuerdo a la información recopilada, el servicio de comunicaciones para Internet se tiene con una empresa local.

17. ¿Quien tiene acceso a Internet?

- Objetivo:

  Conocer si el acceso a Internet comercial esta disponible o no a todos los empleado de la UFG.

- Respuesta:

  Todo el personal tiene acceso a Internet

- Análisis:

  De acuerdo a la fuente entrevista, el cien por ciento de los empleados tiene acceso a Internet, sin importar al área a la que estos pertenezcan.

18. ¿Existe un documento que registre la distribución del equipo y sus usuarios?

- Objetivo:

  Conocer si existe un documento donde se lleve el registro de distribución de equipos y quienes son sus usuarios

- Respuesta:

  Existe un documento.

- Análisis:

  De acuerdo a la respuesta de esta pregunta, se dice que cuentan con un documento que registra cada uno de los activos; pero este documento no se pudo obtener, además cuando se solicito información de la cantidad de equipo y su distribución, no se informo de forma

clara y precisa, por lo que se considera que este documento no existe o no se tiene actualizado.

19. ¿Cuentan con las respectivas licencias del software que utilizan?

- Objetivo:
  Saber si todos los equipos poseen su licenciamiento respectivo para que cumpla con las leyes de derechos de autor.

- Respuesta:
  Si tiene licencias de cada software

- Análisis:
  Según el personal entrevistado, existe licenciamiento de todos los programas y aplicaciones que residen en los equipos.

20. ¿Qué Sistemas Operativos tienen y que software de servidor están instalados en estos?

- Objetivo:
  Saber que versiones de sistemas operativos están instaladas en los equipos con funciones de servidor.

- Respuesta:
  - Windows 2003 => Red local, Sql Server
  - Susse 9.2 => Servidor web y Servidor de Correo electrónico
  - Solares 8 => Base de datos Oracle

- Análisis:
  Se determinó que existen tres diferentes tecnologías de sistemas operativos, los cuales son: Windows 2003, Linux Susse 9.2 y Solaris 8, los cuales son utilizados para soportar aplicaciones de servidor como Base de datos, Servicios Web y Software de red.

21. ¿Poseen Firewall?

- Objetivo:
  Saber si la red local esta protegida de ataques externos por medio de un firewall. Que tipo de Firewall y si posee redundancia el caso de fallar el principal

- Respuesta:
  Si tiene un firewall

- Análisis:

De acuerdo a la información proporcionada por el Administrador de red, se establece que tienen un Firewall, este es a nivel de Software, el nombre del Firewall es Checkpoint y no poseen redundancia

22. ¿Describa las funciones que realiza actualmente el firewall?

- Objetivo:

  Saber las funciones del firewall y analizar que elementos están siendo protegidos

- Respuesta:

  Las funciones son:

  - Habilitación de red para navegación
  - Políticas de Navegación
  - Habilitación y deshabilitación de puertos

- Análisis:

  Se determinaron las funciones del Firewall, pero al investigar con los servicios que ofrece este Firewall, se verifica que esta herramienta tiene una gran gama de funcionalidades adicionales que no menciono el Administrador de red, no se logro determinar si las otras funciones no están siendo utilizadas o si las desconocen.

23. Comente sobre la seguridad del lado del usuario (Desktop)

- Objetivo:
  - Saber que herramientas utilizan para salvaguardar al usuario
  - Cuales son los controles que realiza el administrador de la red
  - Cuales son los problemas de seguridad más comunes de lado del usuario

- Respuesta:
  - Herramienta de protección utilizada: e-Trust(Antivirus) y Firewall de Windows XP
  - Controles: Verificar actualizaciones de aplicaciones, instalación de antivirus.
  - Problemas mas comunes: Virus y Spywers(programas publicitarios no autorizados)
- Análisis:

De acuerdo a la información de esta pregunta, podemos mencionar que la herramienta actualmente utilizada para los desktops es el antivirus e-trust, y el firewall de Windows XP en los equipos que corren sobre sistemas operativos XP.

Los controles realizados son: verificar que el firewall de XP este habilitado y hacer las actualizaciones respectivas en los sistemas operativos.

Los problemas más comunes de seguridad del lado de los desktops son: Virus, programas no autorizados y programas dañinos al sistema.

24. Comente sobre el correo electrónico

- Objetivo:
  - Saber que tipo de correo electrónico tienen
  - Conocer la Herramientas utilizada para la seguridad del correo y sus funciones
  - Saber cuales son los problemas más comunes que se tienen con el servicio de correo electrónico.
  - Conocer si el servidor de correo genera bitácoras.

- Respuesta:
  - Correo electrónico: SendMail
  - Herramienta de seguridad: e-Trust
  - Problemas más comunes: Capacidad de almacenamiento y rendimiento del servidor de correo
  - Genera bitácoras: Si existen

- Análisis:

  De acuerdo a la información proporcionada por el personal entrevistado se mencionó que la herramienta de correo utilizada es SendMail y esta instalado en una versión de linux Suse 9.0.

  La herramienta de seguridad es un antivirus (e-Trust) que filtra tanto el correo entrante como el saliente.

  Los problemas más comunes son: capacidad de almacenamiento y lentitud en el servicio.

  Si hay generación de bitácoras, aunque no se especifica a que nivel

25. Comente sobre el antivirus

- Objetivo:
  - Saber que antivirus posee.
  - Conocer su periodo de actualización.
  - Saber en que equipos se ha instalado.
  - Conocer comentarios sobre la efectividad del mismo.

- Respuesta:
  - Nombre del antivirus: e-Trust de Computer Associate.
  - Periodo de Actualización: Se actualiza en línea a través de Internet cada 24 Hrs.
  - Equipos donde esta instalado: Todos los equipos de la Universidad.
  - Nivel de efectividad: 80%.

- Análisis:

  Con la información obtenida se concluye que el antivirus es e-Trust de Computer Associate, este antivirus es actualizado cada 24 Hrs. Se encuentra instalado en todos los equipos de usuarios finales. Este equipo tiene una consola, la cual se encarga de bajar las actualizaciones a cada uno de los equipos. Existe una efectividad alta alrededor del 80%.

26. Comente sobre la seguridad en la Red.

- Objetivo:
  - Saber si la red es monitoreada constantemente.
  - Conocer que tipo de monitoreo se realiza.
  - Saber que elementos se monitorean en la red.
- Respuesta:
  - Se monitorea la red: Si.
  - Tipo de monitoreo: Gráfico y Ethereal(Herramienta de seguridad gratuita).
  - Elementos que se monitorean: Tráfico que pasa por las interfaces del router y protocolos que pasan a través de los concentradores y switches de la red.

- Análisis:

  Luego de la información proporcionada por el entrevistado se logró determinar lo siguiente: Se cuenta con un programa de monitoreo gráfico corriendo en un servidor Linux que representa el tráfico que pasa por las interfaces del router y el Ethereal monitorea los protocolos que pasan a través de los concentradores y switches de la red.

27. Comente sobre la navegación a Internet

- Objetivo:
  - Saber como es la Navegación a través de que dispositivo es regulada.
  - Saber si existen bitácoras de navegación por usuarios.

- Respuesta:
  - La navegación es controlada por: Proxy.
  - Existen Bitácoras de navegación: Si, por usuario.

- Análisis:

  De acuerdo a los datos proporcionados se dice que: La navegación es controlada por un Proxy. El Proxy es Computer Associate, el cual se llama Etrust Security Manager Content que funciona como Antivirus y Proxy simultáneamente.

  Además existen Bitácoras de navegación por usuario.

28. ¿Cuándo se realizan las actualizaciones de Hardware (HW)?

- Objetivo:

  Saber en que momento se toman decisiones para actualizar el HW, ya sea este parcial o completo.

- Respuesta:

  La actualización de HW se hace de acuerdo a un plan de actualizaciones

- Análisis:

  Según la persona entrevistada las actualizaciones de HW se hacen de acuerdo a un plan de actualizaciones y se llevan a cabo de manera global. No se logro obtener dichos planes.

29. ¿Cuándo se realizan las actualizaciones de Software (SW)?

- Objetivo:

  Saber en que momento se actualiza los SW o Paquetes de SW utilizados por la UFG.

- Respuesta:

  Se actualizan mediante un plan de actualización o cuando se sabe de nuevas versiones de los mismos.

- Análisis:

  Las personas entrevistadas dicen que se realiza de acuerdo a un plan de actualizaciones o cuando saben de nuevas versiones. Se tuvo la misma dificultad que en la pregunta anterior para obtener estos planes que dicen desarrollar.

30. ¿Existe un Inventario de todos los equipos informáticos?

- Objetivo:

  Saber si se llevan un inventario de todos los equipos

- Respuesta:

  Si, existe

- Análisis:

  Según la información de los entrevistados, se cuenta con un inventario de los activos informáticos; pero se pudo evidenciar que este inventario no esta actualizado, ni clasificado eficientemente.

CUESTIONARIO F3 (DIAGNÓSTICO HISTORICO A LOS SISTEMAS DE INFORMACION)

Objetivo general: Conocer sobre la Seguridad Informática implementada durante periodos anteriores, y como esta ha beneficiado a la Institución.

31. Describa como ha cambiado la estructura informática de la Universidad en los últimos años.

- Objetivo:

  Conocer si ha existido algún cambio en la infraestructura de la UFG en los Últimos años y ver hacia donde se dirige desde el punto vista informático.

- Respuesta:
  - Se han adquirido nuevos servidores
  - Se ha incrementado el ancho de banda
  - Se creo UFG TV, para la transmisión de las clases
  - Se ha comprado mas equipo de computo para los Usuarios, alumnos y empleados
  - Compra de Solución de Monitoreo de Red
  - Cambios en la organización, CDSOFT, UFGTV, APTECH

- Análisis:

  De acuerdo a las personas entrevistadas, se ha realizado fuerte inversión de Hardware y Software, mejorando servicios de comunicación. Se ha creado servicios virtuales tales como: UFG TV, Radio UFG. Ha crecido el equipo tecnológico, ahora existen más centros de cómputo y áreas especiales para la navegación y laboratorios especializados de computación y electrónica.

32. ¿Donde ha observado mayor crecimiento tecnológico?

- Objetivo:

  Conocer el área que más se ha visto beneficiada con la tecnología.

- Respuesta:
  - La construcción del Edificio EBLE (Antes Edificio Inteligente)
  - Los Laboratorios del EBLE
  - CDSOFT

- Análisis:

  Según las personas entrevistadas, todos coinciden que el edificio EBLE es el que más beneficio ha alcanzado con la tecnología, tiene las instalaciones más adecuadas para el desarrollo tecnológico. También consideran que ha sido beneficiada la unidad CDSOFT (Centro de Desarrollo de Software).

33. Describa el nivel de mecanización de los procesos actuales en la Universidad y menciona algunos de ellos

- Objetivo:

  Conocer el Nivel de mecanización de los procesos de la Universidad
- Respuesta:
  - Se ha mecanizado casi por completo el sistema de biblioteca (bliblioweb)
  - El sistema de Evaluación Docente
  - Plataforma Virtual para exámenes en línea
  - Sistema de reserva de equipos de computo en línea
  - Laboratorios virtuales de telecomunicaciones
  - Laboratorio GPS
  - Inscripción en línea

- Análisis:

  De acuerdo a la información proporcionada, la Universidad ha mecanizado los procesos más importantes para los estudiantes tales como: Ingreso de nota, inscripción en línea, biblioteca. Además ha desarrollado otros sistemas para apoyo del estudiante como la plataforma virtual, la adquisición de software para laboratorios.

34. ¿Cual ha sido según su experiencia el peor acto de violación a SI en los últimos años y describa como fue?

- Objetivo:
  Saber cual ha sido el mayor sabotaje a la seguridad informática

- Respuesta:
  - Hurto de IP del Servidor de Antivirus
  - Negación de servicio

- Análisis:
  De acuerdo al personal entrevistado, consideran que han existido dos ataques de gran importancia a los sistemas de información. El primero, el hurto de IP del servidor de Antivirus y en segundo lugar la caída de su servidor web o negación de servicio.

35. Comente otros eventos que hayan puesto en riesgo la SI

- Objetivo:
  Profundizar sobre el tema de ataques ocurridos en el pasado a la seguridad informática.

- Respuesta:
  Robo de Equipos de cómputo

- Análisis:
  Según esta información, otro evento sucedido de gran impacto de violación a la seguridad, ha sido el robo de equipo informático.

36. Según su experiencia los problemas anteriores se enfocan principalmente en:

- Objetivo:

Conocer la causa de las debilidades explotadas en el pasado.

- Respuesta:
  Falta de una política de seguridad documentada.

- Análisis:
  De acuerdo a las personas entrevistadas, la falta de una política de seguridad informática es la causa de los problemas a la seguridad.

37. ¿Como se realiza el seguimiento a los avances en términos de Seguridad Informática?

- Objetivo:
  - Saber si existe una persona a cargo de esta actividad
  - Saber como determinan si están mejorando a nivel de seguridad informática

- Respuesta:
  - Existen dos personas a Cargo: Susan Cano y el Ing. Newton Díaz.
  - No hay un proceso formal que de seguimiento a los avances.

- Análisis:
  Se determinó que existen dos personas responsables de la gestión de seguridad, pero que no cuentan con procesos formales para llevar seguimiento a los avances en términos de seguridad informática.

38. ¿Existen proyectos a futuro sobre mejorar la SI?

- Objetivo:
  Saber cuales son los planes futuros alrededor de la Seguridad Informática

- Respuesta:

Si. La actualización del Firewall a versión Hardware y la creación de la política de seguridad

- Análisis:
  Según la información proporcionada, existen proyectos a futuro, específicamente la actualización del firewall a tipo HW y SW y la creación de la política de seguridad.

39. ¿Sabe de algún requerimiento o exigencia hecha a la Universidad por otras Instituciones sobre el tema de SI?

- Objetivo:
  Saber si hay requerimientos de mejora en la seguridad, ya sea requerimientos internos o externos de Instituciones que tenga una relación o alianza con la UFG.

- Respuesta:
  No hay requerimientos

- Análisis:
  De acuerdo a las personas entrevistadas, no se ha realizado ningún tipo de requerimientos en materia de seguridad informática por parte de Instituciones nacionales o internacionales.

CUESTIONARIO F4 (DIAGNÓSTICO A LOS SISTEMAS DE INFORMACION)

Objetivo general: Conocer sobre el tratamiento a los sistemas de información, procesos de desarrollo de sistemas, mantenimiento y otros aspectos relevantes en el área de informática.

40. ¿Que motores de bases de datos utilizan para la gestión de la información de los sistemas críticos internos?

- Objetivo:

Conocer los motores de bases de datos utilizados en los sistemas críticos internos de La Universidad.

- Respuesta:
  Sql Server de Microsoft

- Análisis:
  De acuerdo a la información proporcionada, el motor de base de datos para el almacenamiento de información de los sistemas críticos, es: SQL Server, utilizan Oracle pero solo para usos didácticos.

41. ¿Existen manuales de usuario y técnico de las aplicaciones internas?

- Objetivo:
  Verificar si actualmente la Universidad cuenta con manuales de usuario y técnico de las aplicaciones internas.

- Respuesta:
  Si

- Análisis:
  Según las personas entrevistadas, Administración académica si cuenta con manuales de los sistemas internos, pero no así los sistemas desarrollados por el departamento de tecnología y comunicaciones. No se pudo obtener copias de estos manuales

42. ¿Los sistemas críticos (notas, expediente académico, otros) controlan el ingreso de cada usuario?

- Objetivo:
  Conocer si actualmente la Universidad cuenta con controles de ingreso de usuarios a los sistemas críticos.

- Respuesta:

  Si es controlado el ingreso a los sistemas críticos por medio de la identificación del usuario.

- Análisis:

  Se determinó, que los ingresos a los sistemas son a través de claves de acceso.

43. ¿Existen controles de las actividades (bitácoras) que realiza el usuario cuando esta dentro de los Sistemas?

- Objetivo:

  Conocer si actualmente la Universidad cuenta con bitácoras que controlen las actividades que realizan los usuarios dentro de los sistemas.

- Respuesta:

  Si se realizan controles de las actividades que llevan a cabo los usuarios dentro del sistema.

- Análisis:

  Según la información proporcionada, los controles de las actividades de los usuarios dentro del sistema son almacenados por medio de fecha, acción que realiza y por medio de una identificación de usuario.

44. ¿Existen procesos de Backup (copias de seguridad) de los bancos de información?

- Objetivo:

  Verificar si la universidad realiza backup de los bancos de información.

- Respuesta:

  Si se realizan copias de seguridad de la información y estos son realizados a diario.

- Análisis:

De acuerdo a las personas entrevistadas, si realizan copias de seguridad y se llevan a cabo todos los días. Además existe un responsable de esta actividad.

45. ¿Como se garantizan la realización y efectividad de los backups?

- Objetivo:
  Verificar la realización y efectividad de los backups de los bancos de información.

- Respuesta:
  Se verifican periódicamente.

- Análisis:
  De acuerdo a la respuesta proporcionada, las revisiones a las copias de respaldo son hechas de forma manual y se lleva a cabo de forma periódica.

46. ¿Cuentan con un plan de contingencia que cubra problemas por pérdida o robo de información?

- Objetivo:
  Conocer si la universidad posee planes de continencia por perdidas, fraudes o robo de la información.

- Respuesta:
  No.

- Análisis:
  De acuerdo a la información proporcionada, no se tiene un documento o plan de contingencia; si cuentan con medidas básicas de seguridad como las copias de respaldo.

47. ¿Que controles se efectúan sobre los usuarios responsables de alimentar los sistemas de información?

- Objetivo:
  Identificar los controles que se realizan sobre los usuarios que alimentan los sistemas de información.

- Respuesta:
  - Se lleva a cabo un control de bitácora.
  - Se llevan políticas de acceso a los sistemas.

- Análisis:

  Según el personal entrevistado, se realizan controles a través de bitácoras en los sistemas, además los sistemas controlan los permisos de acceso de los usuarios.

48. ¿Los sistemas que funcionan en un entorno Web pueden ser alimentados fuera de la universidad?

- Objetivo:

  Identificar si los sistemas vía Internet pueden ser utilizados desde cualquier lugar.

- Respuesta:

  Si pueden ser alimentados fuera de la Universidad

- Análisis:

  La información proporcionada, especifica que no existe restricción para el uso del sistema de ingreso de notas o cualquier otra que trabaje a través de Internet, siempre y cuando tenga el usuario y clave autorizada puede utilizar estos sistemas.

49. ¿Las conexiones vía Internet utilizan algún proceso de seguridad?

- Objetivo:

  Establecer el nivel de seguridad de las conexiones vía Internet que utiliza la universidad para sus aplicaciones web.

- Respuesta:

  Los procesos de seguridad vía Internet que utiliza son de tipo SSL.

- Análisis:

De acuerdo al personal entrevistado, las conexiones que la universidad utiliza para seguridad de aplicaciones web es SSL (Socket Secure Layer) conexiones con capa de seguridad. Esta información fue verificada; pero las aplicaciones no respondieron bajo los puertos 4433 o sobre el protocolo HTTPS en el cual se aplica el SSL, por lo que se determina que no utilizan capas de seguridad vía Internet.

50. ¿Existe una sola base de datos centralizada de la información académica de los estudiantes (notas, expediente académico, etc.)?

- Objetivo:
  Identificar la organización de la base de datos que Administración Académica utiliza para su banco de información.

- Respuesta:
  Al consultar algunas autoridades contestaron que si y otras que no.

- Análisis:
  De acuerdo a la información proporcionada, existen contradicciones con respecto a que existe una base de datos centralizada, por lo que se considera que esto es falso y que posiblemente existan copias de la base de datos trabajando con otras aplicaciones. Esta información no fue posible verificar, por falta de autorización.

51. ¿Que controles se aplican a los sistemas que hacen uso de la información de los estudiantes?

- Objetivo:
  Conocer si existen controles sobre las aplicaciones que interactúan con la base de datos de notas y expediente de estudiantes.

- Respuesta:
  Existen controles a nivel de permisos que se dan a estas aplicaciones. Lectura, Actualización.

- Análisis:

  La información proporcionada, determinó que las aplicaciones que hacen uso de los bancos de información críticos son controlados a nivel de los permisos que tienen configurados, estos podrían ser: Solo lectura, Actualización, Inserción, Eliminación.

52. ¿Existen controles para garantizar la integridad y calidad de la información que esta almacenada?

- Objetivo:

  Verificar que la integridad y calidad de la información que se almacena es correcta.

- Respuesta:

  Los controles son de integridad relacional, a nivel de base de datos y en las aplicaciones.

- Análisis:

  De acuerdo al personal entrevistado, existe validación de la integridad a nivel de base de datos y sobre las aplicaciones.

53. ¿Los proyectos de nuevas aplicaciones son ejecutados por?

- Objetivo:

  Identificar que las personas que están a cargo de las nuevas aplicaciones sean las más adecuadas.

- Respuesta:

  Personal técnico.

- Análisis:

  De acuerdo a la información proporcionada, las aplicaciones son desarrolladas por personal técnico que labora en la institución, descartando a estudiantes, o subcontratación de servicios. Existe un departamento a cargo de esta actividad.

54. ¿Cuando se realizan modificaciones a los programas a iniciativa de quien es?

- Objetivo:
  Determinar que personas son las involucradas en los procesos de mantenimiento a los sistemas.

- Respuesta:
  Usuarios, programadores, director de informática.

- Análisis:
  La información de los entrevistados, determinó que las tres fuentes principales que dan origen a que se realicen mantenimientos en los sistemas son: Usuarios, programadores y director de informática.

55. ¿Existe algún contrato o documento de confidencialidad acordado con los empleados de la universidad?

- Objetivo:
  Conocer si la Universidad establece contratos de confidencialidad con su personal.

- Respuesta:
  No existe un contrato o documento de confidencialidad para los empleados.

- Análisis:
  De acuerdo al personal entrevistado, nunca han firmado convenios de confidencialidad o cualquier documento de carácter legal.

CUESTIONARIO F5 (DIAGNOSTICO A LA SEGURIDAD FISICA Y LOGICA)

Objetivo general: Conocer los niveles de seguridad implementados a nivel físico y lógico.

56. ¿Existe una persona responsable de la seguridad física en la universidad?

- Objetivo:
  Identificar quien es el encargado de la seguridad física de la universidad.

- Respuesta:
  Si existe, labora en la Unidad de tecnología y comunicaciones.

- Análisis:
  Según la información de los entrevistados, si existe una persona a cargo de la seguridad informática de la Universidad, la cual labora en el departamento de tecnología y comunicaciones.

57. ¿Existen controles de trabajo fuera de horario normal?

- Objetivo:
  Verificar que se pidan los permisos respectivos para laborar fuera de horas de laborales.

- Respuesta:
  Si existen controles fuera de horario de trabajo.

- Análisis:
  De acuerdo a la información obtenida, se determinó que para poder trabajar fuera de horario laboral se necesita autorización del jefe inmediato.

58. ¿Se controlan los accesos físicos al lugar donde están los servidores de BD y comunicaciones?

- Objetivo:
  Conocer como se controlan los accesos físicos a los servidores de BD, aplicaciones y comunicaciones.

- Respuesta:
  Los controles son humanos.

- Análisis:

  De acuerdo a las personas entrevistadas, únicamente existen controles humanos, verificando que la persona que ingresa trabaje en la Institución, esto por los mismos empleados del área.

59. ¿Para ingresar físicamente a estos lugares críticos, se necesita?

- Objetivo:

  Conocer que medios utiliza la Universidad para el acceso físico a las instalaciones de los servidores de BD y comunicaciones.

- Respuesta:

  Con solo abrir la puerta adonde se encuentran estos equipos es suficiente para ingresar a las instalaciones.

- Análisis:

  Se determino que no cuentan con procesos de control físico que permita verificar quien y cuando ingresa. Los accesos son los mas básicos posibles, a través de puertas.

60. ¿Existe vigilancia permanente en el centro de cómputo y administración académica las 24 horas?

- Objetivo:

  Verificar que estas áreas o departamentos se encuentren en constante vigilancia.

- Respuesta:

  No son vigilados las 24 horas estos departamentos.

- Análisis:

  Tomando la respuesta proporcionada, se determina que la vigilancia es a nivel del ingreso al campus universitario; pero no se realiza vigilancia al interior de las unidades de

Administración Académica o Tecnología y Comunicaciones en horarios nocturnos o no laborales.

61. ¿En el Centro de Cómputo y Administración Académica existen alarmas?

- Objetivo:
  Identificar si existen alarmas y de que tipos son.

- Respuesta:
  La universidad no cuenta con alarmas para detectar fuego, detector de movimientos, fugas de agua, etc.

- Análisis:
  De acuerdo al personal entrevistado, no se cuenta con ningún tipo de alarma al interior de las unidades de Administración académica o Tecnología y comunicaciones.

62. ¿Existen extintores de fuego?

- Objetivo:
  Conocer si cuenta con equipo básico de protección contra incendios.

- Respuesta:
  Si se cuenta con extintores de fuego.

- Análisis:
  La universidad cuenta con extintores de fuego y el personal esta capacitado para poder manejarlos a la hora de que exista una emergencia, estos extintores son manuales.

63. ¿Las conexiones de energía y red están etiquetadas?

- Objetivo:
  Conocer si existe orden alrededor de puntos de red y conexiones eléctricas.

- Respuesta:

Si se tienen etiquetadas las conexiones de red y energía

- Análisis:

  Todas las personas encuestadas coinciden que si se tienen etiquetadas las conexiones de red y energía, y estos están conectados a un UPS central; dichas conexiones eléctricas están polarizadas respectivamente.

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

- Objetivo:

  Verificar que el personal este informado de que hacer a la hora de una emergencia.

- Respuesta:

  Si esta capacitado todo el personal.

- Análisis:

  De acuerdo a la información proporcionada, se determinó que el personal ha sido capacitado en caso de emergencias como terremotos.

65. ¿Explique la forma en que se protegen físicamente las copias de seguridad (caja de seguridad, archivos, bóvedas)?

- Objetivo:

  Conocer la forma de proteger físicamente las copias de seguridad de los sistemas de información.

- Respuesta:

  Se guardan una copia general de las BD en un banco local.

- Análisis:

  Según el personal entrevistado, se guarda una copia general en un banco no especificado; esta información no fue posible verificarla por no tener documentación que respalde dicha actividad.

66. ¿Existe un contrato de seguro para los equipo de computo?

- Objetivo:

  Definir que los equipos estén debidamente respaldados por seguros.

- Respuesta:

  No cuentan con un seguro para los equipos.

- Análisis:

  Según el personal entrevistado, contratos de seguros no existen, cuentan con garantías que los proveedores dan por la compra de equipos.

67. ¿La navegación a Internet de los alumnos y empleados es controlada y monitoreada?

- Objetivo:

  Controlar el tipo de usuario que utiliza la red de la universidad.

- Respuesta:

  Si son controlados y monitoreados.

- Análisis:

  De acuerdo a la información obtenida, se dice que si son controlados y monitoreados los alumnos y empleados de la universidad; también las conexiones inalámbricas son controladas.

68. ¿Existe un control y revisión de los programas que están instalados y como están configurados los equipos?

- Objetivo:

  Verificar que los controles y revisiones de los programas y configuraciones de los equipos sea la establecida por el área a cargo de estas tareas.

- Respuesta:

Si, se controlan y revisan los programas, así como sus respectivas configuraciones y es de tipo manual.

- Análisis:

  De acuerdo a las personas entrevistas, los controles de los programas instalados en cada equipo se hacen de forma manual, no cuentan con software a cargo de realizar esta actividad de forma automatizada. Además se hace de forma periódica pero sin ningún plan establecido.

69. ¿Existe una persona a cargo de la administración de la seguridad del centro de cómputo?

- Objetivo:

  Identificar a la persona encargada de salvaguardar la administración del centro de cómputo.

- Respuesta:

  Si existe

- Análisis:

  Según la dirección de tecnología y comunicaciones, recientemente se ha contratado a una persona específicamente para esta labor de seguridad.

70. ¿Existe redundancia en servidores y sistemas de comunicación?

- Objetivo:

  Conocer si la Universidad cuenta con equipos de respaldo

- Respuesta:

  No.

- Análisis:

  De acuerdo al personal técnico, la Institución no cuenta con equipo de respaldo a nivel de servidores y comunicaciones.

71. ¿Existen procesos de mantenimiento preventivo para los equipos de cómputo?

- Objetivo:

  Verificar que la universidad este llevando a cabo mantenimientos preventivos a sus equipos de cómputo.

- Respuesta:

  Si se hacen mantenimientos preventivos y se realizan cada trimestre.

- Análisis:

  Según la información obtenida, se realizan mantenimientos preventivos cada tres meses.

72. ¿Se capacita a los profesores para el ingreso de las notas?

- Objetivo:

  Conocer si los profesores reciben el conocimiento necesario para el ingreso de notas.

- Respuesta:

  Si se capacita a los profesores.

- Análisis:

  De acuerdo a este resultado, se determinó que los profesores reciben capacitación en el uso de los sistemas de ingreso de notas.

73. ¿Existe un control de acceso que cancele el proceso al tercer intento fallido?

- Objetivo:

  Verificar si existen controles básicos para el ingreso a los sistemas.

- Respuesta:

  No se cuenta con un control que cancele el acceso, ni tampoco se lleva un control de intentos fallidos.

- Análisis:

  Según los entrevistados, no se llevan controles de los intentos de ingreso a los sistemas, ni tampoco se cancela al tercer intento.

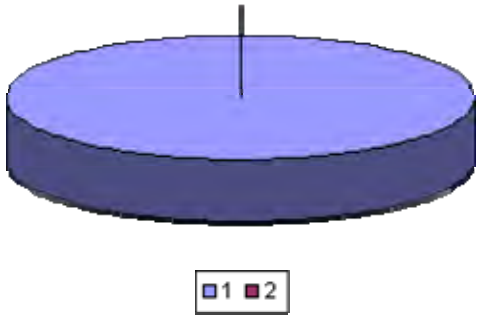
CUESTIONARIO F6 (DIAGNÓSTICO AL NIVEL DE ACEPTACION DEL PROYECTO)

Objetivo General: Conocer la aceptación del recurso humano de la Universidad hacia la implementación de este proyecto, esto como parte del análisis de estudio de factibilidad.

74. ¿Estaría interesado en una herramienta que les facilite llevar un mejor control sobre La Seguridad Informática?

Objetivo pregunta:
Identificar el grado de interés por parte del personal de la UFG en llevar controles sobre la seguridad informática.

Datos de clasificación	**PUESTO DE TRABAJO**							
	JEFATURA		**TECNICA**		**ADMINISTRATIVA**			
Alternativas	Fr	%	Fr	%	Fr	%	FR	%
1. Si	3	100	4	100	4	100	11	100
2. No	0	0	0	0	0	0	0	0
Totales	3	100	4	100	4	100	11	100

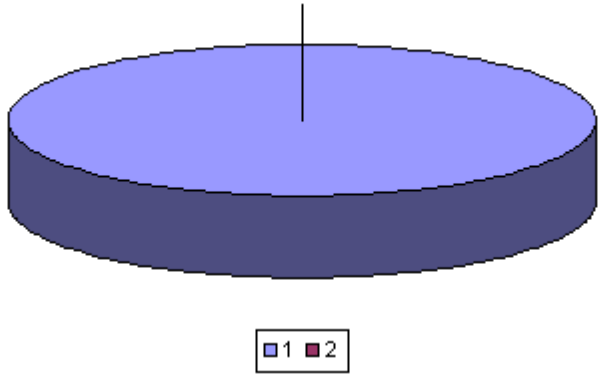


Análisis:
De acuerdo a los resultados obtenidos, el 100% del personal esta interesado en una herramienta que les sirva para llevar un control más exacto y preciso de la seguridad informática de La UFG.

75. ¿Le parecería que la herramienta sea accesible a través de un navegador de Internet (Browser)?

Objetivo pregunta:
Definir si el ambiente web es el entorno más adecuado para correr el sistema.

Datos de clasificación	**PUESTO DE TRABAJO**							
	JEFATURA		**TECNICA**		**ADMINISTRATIVA**		FR	%
Alternativas	Fr	%	Fr	%	Fr	%		
1. Si	3	100	4	100	4	100	11	100
2. No	0	0	0	0	0	0	0	0
Totales	3	100	4	100	4	100	11	100

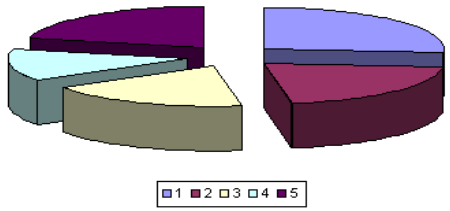


Análisis:
Todos los entrevistados coinciden que les gustaría una herramienta de tipo Web para trabajar a través de un navegador Web.

76. ¿Qué elementos le gustaría que la herramienta le brindara'?

Objetivo pregunta:
Identificar cual es la demanda actual de los usuarios para la construcción de la herramienta para la seguridad informática.

Datos de clasificación	**PUESTO DE TRABAJO**							
	JEFATURA		**TECNICA**		**ADMINISTRATIVA**			
Alternativas	Fr	%	Fr	%	Fr	%	FR	%
1. Elaboración de informes electrónicos	3	20	4	28.57	3	33.33	10	26.32
2. Detalle de la situación actual en cumplimiento de la política de seguridad	3	20	3	21.43	2	22.22	8	21.05
3. La norma documentada	3	20	2	14.29	2	22.22	7	18.42
4. Base de conocimientos	3	20	1	7.14	1	11.11	5	13.16
5. Evaluaciones sobre seguridad informática	3	20	4	28.57	1	11.11	8	21.05
Totales	15	100	14	100.00	9	100.00	38	100.00

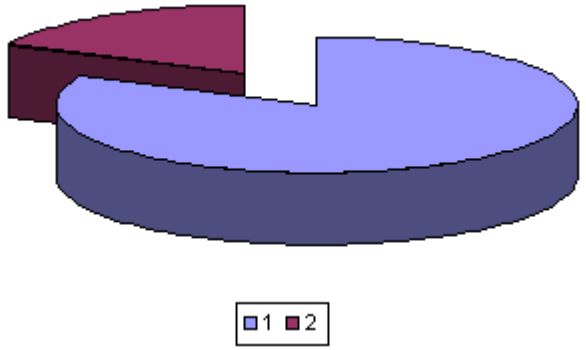


Análisis:
Según la opinión de los usuarios, las alternativas que poseen mayor ponderación es la elaboración de informes electrónicos con un 26.32%, luego tenemos que el detalle de la situación actual y evaluaciones sobre seguridad informática con un 21.05% cada una, y los otros porcentajes se distribuyen en las opciones de la norma documentada y la base de conocimientos.

77. ¿Estaría dispuesto a colaborar con el diseño para el desarrollo de la herramienta?

Objetivo pregunta:
Identificar el grado de aceptación y colaboración por parte de los usuarios.

Datos de clasificación	**PUESTO DE TRABAJO**							
	JEFATURA		**TECNICA**		**ADMINISTRATIVA**			
Alternativas	Fr	%	Fr	%	Fr	%	FR	%
Si	3	100	2	50	4	100	9	82
No	0	0	2	50	0	0	2	18
Totales	3	100	4	100	4	100	11	100



Análisis:
La mayoría de los entrevistados con un 82% esta de acuerdo en ayudar o facilitar la información pertinente para el desarrollo del sistema, el resto contesto que no podría ayudar con el proyecto.

ANEXO C

SELECCIÓN DE PLATAFORMA DE DESARROLLO

Esta actividad se llevo acabo para sustentar la decisión de la tecnología web utilizada en el proyecto. El proceso consiste, en estudiar una serie de variables importantes y compararla contra las diferentes tecnologías consideraras para el desarrollo del software, a través de este estudio se logró identificar aquella plataforma que mejor rendimiento le ofrece al sistema y se adecue a la tecnología utilizada por la Universidad.

Aspectos a tener en cuenta en un lenguaje de scripts

Existen una serie de características a considerar para tomar la decisión de que plataforma utilizar en aplicaciones para ambiente web, a continuación se presentan las mas importantes.

- **Velocidad:** No solo la velocidad de ejecución, la cual es importante, sino además no crear demoras en la máquina. Por esta razón no debe requerir demasiados recursos de sistema.
- **Estabilidad:** La velocidad no sirve de mucho si el sistema se cae cada cierta cantidad de ejecuciones. Ninguna aplicación es 100% libre de bugs, pero teniendo de respaldo una increíble comunidad de programadores y usuarios es mucho mas difícil para lo bugs sobrevivir.
- **Seguridad:** El sistema debe poseer protecciones contra ataques.
- **Simplicidad:** Se les debe permitir a los programadores generar código productivamente en el menor tiempo posible.
- **Conectividad:** Colaboración con otras aplicaciones, facilidad para interactuar en diferentes plataformas y ambientes.
- **Manejo de errores:** Ayuda para el programador a la hora de identificar y controlar errores de diferente naturaleza.
- **Entorno de desarrollo**: Un ambiente de desarrollo que permita de forma rápida y sencilla la utilización de los recursos que ofrece el lenguaje.
- **Precio**: La inversión monetaria a realizar para aplicar dicha tecnología.

- **Soporte:** Apoyo por expertos en el área, facilidad para encontrar soluciones a problemas.
- **Plataformas:** El sistema debe poderse implementar en diferentes ambientes de servidores web y sistemas operativos.

Lenguajes de scripts seleccionados para el estudio:

ASP.Net, PHP, JSP (Estos lenguajes son revisadas detalladamente en el capitulo 1 y apartado "Antecedentes tecnológicos relacionados con el proyecto")

A continuación se presenta una tabla comparativa de cada uno de los lenguajes scripts y la forma de tratar las variables mencionadas anteriormente.

VARIABLE	PHP 5	ASP.NET	JSP
Velocidad	Alta	Baja	Media
Estabilidad	Fuerte	Débil	Fuerte
Seguridad	Alta	Alta	Alta
Simplicidad	Alta	Alta	Media
Conectividad	Alta	Baja	Alta
Manejo de errores	Alta	Alta	Alta
Entorno de desarrollo	Alta	Alta	Alta
Precio Software	Gratis	Gratis	Gratis
Precio Plataforma	Gratis	Costo Licencias	Gratis
Soporte	Alto	Alto	Alto
Plataforma Servidor Web	Fuerte	Baja(IIS, Win)	Fuerte
Plataformas Sistema Operativo	Muchas	win32 (IIS unicamente)	Muchas

Tabla: Comparación de lenguajes scripts [1]

Análisis de resultados

Se puede observar que los lenguajes mejor evaluados son PHP y JSP, superando fácilmente a ASP.NET.

[1] http://www.oracle.com/technology/pub/articles/hull_asp.html

Se presenta a continuación referencias sobre estas tecnologías y otros estudios realizados por compañías de tecnología.

Funcionamiento benchmarking (comparación de productos) PHP, ASP, JSP, Coldfusion

Referencia: http://aldev0.virtualave.net/php-perl-benchmarks.html

El Zdnet[2] hizo una evaluación y benchmarking de 4 lenguajes de scripting de la web.

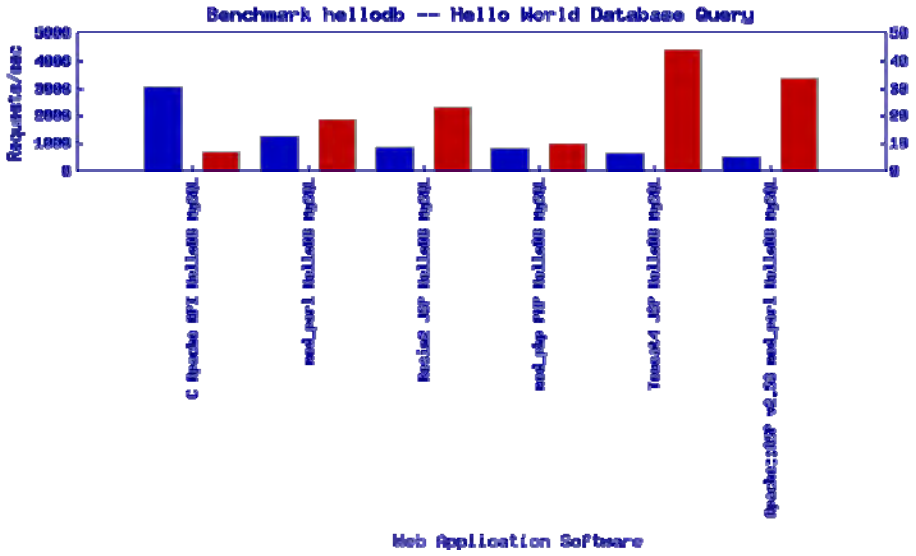
Durante este estudio, se utilizaron ambientes idénticos, el CPU y memoria fueron bajo condiciones idénticas.

Se encontró que PHP era cerca de 3,7 veces más rápido que JSP y cerca de 1,2 veces más rápido que la ejecución de ASP.

- PHP resolvió 47 paginas/segundo
- Microsoft ASP resolvió 43 paginas/segundo
- Allaire ColdFusion 29 paginas/segundo
- Java JSP 13 paginas/segundo

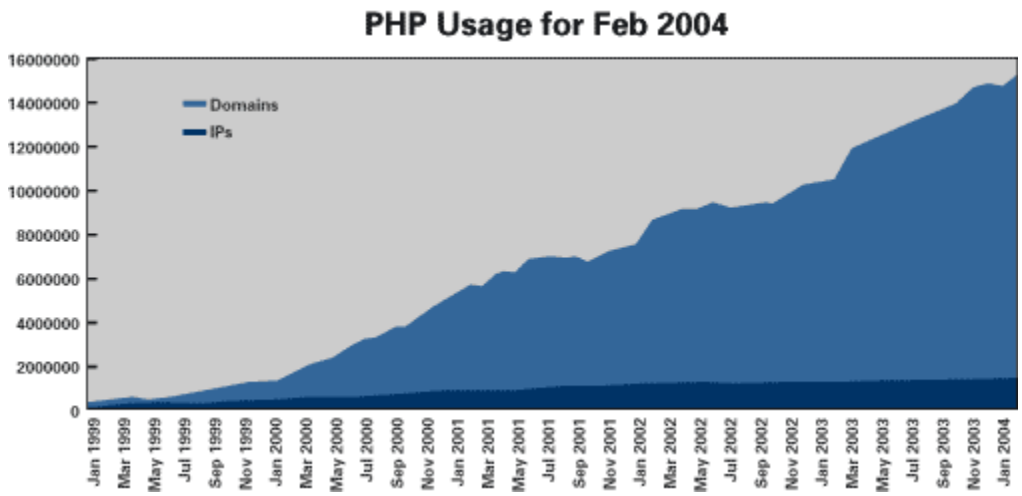
Rendimiento de Aplicaciones Web

Referencias: http://db.ilug-bom.org.in/Documentation/HOWTO/PHP-HOWTO-13.html



[2] http://www.zdnet.com/ Revista especializada en tecnología

Crecimiento de la plataforma PHP durante el año 2004
Referencia:
http://www.programacion.com/blogs/60phpland/archive/292phpvsaspfacilidad_portabilidad_precio_velocidad_y_mas.html



Recursos tecnológicos de la Universidad Francisco Gavidia

Características de WebServer

Hadware	**Especificación**
Procesador	Intel Xeon 2.8ghz
Memoria Primaria	2GB DDR ECC REG
Memoria Secundaria	Discos duros de 73GB ultra 320 SCSI 10.000 rpm
Tarjeta de red	100 Mbps
Software	Especificación
Servidor Web	Apache
Sistema Operativo	Linux Suse 9.0
Base de datos	Mysql, Postgress
Módulos	Php, Perl, C++

Resultado final

Se concluye determinando que PHP es la mejor tecnología de lenguaje script para este proyecto, el cual ofrece mejor rendimiento y oportunidad de crecimiento.

Este resultado se puede complementar con la factibilidad técnica presentada en el capitulo 3 y dar por sustentado que la tecnología más recomendada para el desarrollo del software “Sistema automatizado para la ejecución de una auditoria informática aplicando una norma internacional,

caso de estudio norma ISO/IEC 17799:2000 en la sede central de la Universidad Francisco Gavidia" es en definitiva PHP.

Descripción especifica del funcionamiento de PHP y variables importantes de los lenguajes de scripts en entornos web.

- **Velocidad:** PHP se integra muy bien junto a otro software, especialmente bajo ambientes Unix, cuando se configura como módulo de Apache, esta listo para ser utilizado.
- **Estabilidad:** PHP utiliza su propio sistema de administración de recursos y dispone de un sofisticado método de manejo de variables, conformando un sistema robusto y estable.
- **Seguridad:** PHP provee diferentes niveles de seguridad, estos pueden ser configurados desde el archivo .ini
- **Simplicidad:** Usuarios con experiencia en C y C++ podrán utilizar PHP rápidamente.
- **Conectividad:** PHP dispone de una amplia gama de librerías, y agregarle extensiones es muy fácil. Esto le permite al PHP ser utilizado en muchas áreas diferentes, tales como encriptado, gráficos, XML y otras.
- **Manejo de errores:** El manejo de errores no es tan sofisticado como Cold Fusion o ASP.
- **Entorno de desarrollo**: Un debugger ha sido desarrollado por Zend Tech.

ANEXO D

GLOSARIO DE TERMINOS, AUDITORIA, SEGURIDAD INFORMATICA

TERMINOS DE AUDITORIA

Auditor: Persona capacitada para realizar auditorias en empresas u otras instituciones.

Auditoría: Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoria, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razón habilidad de sus resultados y el cumplimiento de sus operaciones.

Auditoría administrativa: Es la revisión sistemática y exhaustiva que se realiza a la actividad administrativa de una empresa, en cuanto a su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades que regulan sus operaciones.

Auditoría Externa: Es la revisión independiente que realiza un profesional de la auditoria, con total libertad de criterio y sin ninguna influencia, con el propósito de evaluar el desempeño de actividades, operaciones y funciones que se realizan en la empresa que lo contrata, así como la razón habilidad en la emisión de sus resultados financieros.

Auditoría Integral: Es la ejecución de exámenes estructurados de programas, organizaciones, actividades o segmentos operativos de una entidad pública o privada, con el propósito de medir e informar sobre la utilización, de manera económica y eficiente de sus recursos y el logro de sus objetivos previstos.

Auditoría Interna o de Campo: Es la revisión que realiza un profesional de la auditoria, cuya relación de trabajo es directa y subordinada a la institución donde se aplicará la misma, con el propósito de evaluar en forma interna el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, así como evaluar la razón habilidad en la emisión de sus resultados financieros.

Auditoría Financiera (contable): Es la revisión sistemática, explorativa y crítica que realiza un profesional de la contabilidad a los libros y documentos contables, a los controles y registros de las operaciones financieras y a la emisión de los estados financieros de una empresa, con el fin de evaluar y opinar sobre la razón habilidad, veracidad, confiabilidad y oportunidad en la emisión de los resultados financieros obtenidos durante un periodo especifico o un ejercicio fiscal.

Auditoría Fiscal :La auditoría fiscal es el proceso sistemático de obtener y evaluar objetivamente la evidencia acerca de las afirmaciones y hechos relacionados con actos y acontecimientos de carácter tributario, a fin de evaluar tales declaraciones a la luz de los criterios establecidos y comunicar el resultado a las partes interesadas; ello implica verificar la razonabilidad con que la entidad ha registrado la contabilización de las operaciones resultantes de sus relaciones con el Ministerio de Hacienda.

Auditoría Operacional: Es la revisión exhaustiva, sistemática y especifica que se realiza a las actividades de una empresa, con el fin de evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo de sus operaciones, cualesquiera que éstas sean, tanto en el establecimiento y cumplimiento de los métodos, técnicas y procedimientos de trabajo necesarios para el desarrollo de sus operaciones, en coordinación con los recursos disponibles, como en las normas, políticas, lineamientos y capacitación que regulan el buen funcionamiento de la empresa.

Auditoría integral: Es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, con el propósito de evaluar, de manera integral, el correcto desarrollo de las funciones en todas sus áreas administrativas, cualesquiera que éstas sean, así como de evaluar sus resultados conjuntos y relaciones de trabajo, comunicaciones y procedimientos interrelacionados que regulan la realización de las actividades compartidas para alcanzar el objetivo institucional; dicha revisión se lleva a cabo también normas, políticas y lineamientos sobre el uso de todos los recursos de la empresa.

Auditoría Gubernamental: Es la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones de una entidad gubernamental, cualquiera que sea la naturaleza de las dependencias y entidades de la Administración Pública Federal.

Auditoría Informática: Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes.

Auditoría de gestión: Es un examen objetivo, sistemático y profesional de evidencias, realizado con el fin de proporcionar una evaluación independiente sobre el desempeño de una entidad, programa o proyecto orientada a mejorar la efectividad, eficiencia y economía en el logro de las metas programadas y en el uso de los recursos públicos para facilitar la toma de decisiones por quienes son responsables de adoptar acciones correctivas y mejorar su responsabilidad ante el público.

Actividades de control gerencial: Se refieren a las acciones que realiza la gerencia y otro personal de la entidad para cumplir diariamente con las funciones asignadas. Son importantes porque en sí mismas implican la forma correcta de hacer las cosas, así como también porque el dictado de políticas y procedimientos y la evaluación de su cumplimiento, constituyen el medio más idóneo para asegurar el logro de objetivos de la entidad.

Alcance: Implica la selección de aquellas áreas o asuntos que serán revisados a profundidad en la fase de ejecución. Esta decisión debe ser efectuada teniendo en cuenta la materialidad, sensibilidad, riesgo, factibilidad y costo, así como la trascendencia de los posibles resultados a informar.

Ambiente de Control Interno: Se refiere al establecimiento de un entorno que estimule e influencie las tareas de las personas con respecto al control de sus actividades. Como el personal resulta ser la esencia de cualquier entidad, sus atributos constituyen el motor que la conduce y la base sobre la que todo descansa. Los factores del ambiente interno de control son:

- integridad y valores éticos

- asignación de autoridad y responsabilidad
- estructura organizacional
- política de administración de personal
- responsabilidad
- clima de confianza en el trabajo

Áreas generales de revisión: Son aquellos asuntos seleccionados en esta etapa de la auditoria. Tales áreas están referidas a:

- Protección y control de recursos públicos.
- Cumplimiento de leyes, normas y regulaciones aplicables.
- Economía y eficiencia.
- Procedimientos para medir e informar sobre la efectividad el programa o actividad.
- Evaluación del programa o actividad.
- Procesamiento y control del sistema de administración financiera y el sistema de información computarizada-SIC.
- Auditoria interna.

Asuntos más importantes: Representan aquellas actividades clave de los sistemas y controles aplicados que, de acuerdo a la opinión del auditor, resultan vitales para el éxito del ente a ser examinada. Constituyen asuntos que tienen importancia en esta etapa, pero que deben ser examinados y confirmados en la fase de ejecución de la auditoria.

Carta de representación: Documento mediante el cual el nivel competente de la entidad examinada reconoce haber puesto a disposición del auditor toda la información requerida, así como cualquier hecho significativo ocurrido durante el período bajo examen. Si se ha examinado varias áreas de la entidad, deberá recabarse varias cartas de representación.

Causa: Representa la razón básica (o las razones) por la cual ocurrió la condición, o también el motivo del incumplimiento del criterio o norma. La simple expresión en el informe de que el problema existe, porque alguien no cumplió apropiadamente con las normas, es insuficiente para convencer al usuario del informe.

Condición: Comprende la situación actual encontrada por el auditor al examinar una área, actividad u transacción. La condición, entendida como **lo que e**s, refleja la manera en que el criterio está siendo logrado. Es importante que la condición haga referencia directa al criterio, en vista que su propósito es describir el comportamiento de la entidad auditada en el logro de las metas expresadas como criterios.

Conclusiones: Son juicios del auditor, de carácter profesional, basados en las observaciones formuladas como resultado del examen. Estarán referidas a la evaluación de la gestión en la entidad examinada, en cuanto al logro de las metas y objetivos, utilización de los recursos públicos, en términos de eficiencia y economía y cumplimiento de la normativa legal.

Controles: Medios a través de los cuales la gerencia de una entidad asegura que el sistema es efectivo y es manejado en armonía con eficiencia y economía, dentro del marco legal vigente.

Control de calidad: Conjunto de métodos y procedimientos implementados dentro de la Contraloría General de la República u otra entidad auditora para obtener seguridad razonable que la auditoria llevada a cabo y el informe correspondiente cumplen con las Normas de Auditoria Gubernamental.

Control Interno: Es un proceso continuo realizado por la dirección y gerencia y, el personal de la entidad; para proporcionar seguridad razonable, respecto a sí están lográndose los objetivos de control interno siguientes:

- Promover la efectividad, eficiencia y economía en las operaciones y, la calidad en los servicios que debe brindar cada entidad pública.
- Proteger y conservar los recursos públicos contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.
- Cumplir las leyes, reglamentos y otras normas gubernamentales.
- Elaborar información financiera válida y confiable, presentada con oportunidad.

Control interno financiero: Comprende el plan de organización y los métodos, procedimientos y registros que tienen relación con la custodia de recursos, al igual que con la exactitud,

confiabilidad y oportunidad en la presentación de información financiera, principalmente, los estados financieros de la entidad o programa.

Control interno gerencial: Comprende el plan de organización, política, procedimientos y prácticas utilizadas para administrar las operaciones en una entidad o programa y asegurar el cumplimiento de las metas establecidas, así como los sistemas para medir, presentar informes y monitorear la ejecución de los programas.

Comunicación: Implica proporcionar un apropiado entendimiento sobre los roles y responsabilidades individuales involucradas en el control interno de la información financiera dentro de una entidad.

Criterios de auditoria: Comprende la norma con la cual el auditor mide la condición. Es también la meta que la entidad está tratando de alcanzar o representa la unidad de medida que permite la evaluación de la condición actual. Igualmente, se denomina criterio a la norma t

Economía: La economía está relacionada con los términos y condiciones en los cuales se adquiere recursos, sean éstos financieros, humanos, físicos o de sistemas computarizados, obteniendo la cantidad y nivel apropiado de calidad, al menor costo, en la oportunidad requerida y en el lugar apropiado.

Ejecución (fase): Fase de la auditoria de gestión focalizada, básicamente, en la obtención de evidencia suficiente y competente sobre los asuntos significativos (líneas de auditoria) aprobados en el plan de auditoria.

Efectividad: Se refiere al grado en el cual un programa o actividad logra sus objetivos y metas u otros beneficios que pretendían alcanzarse, previstos en la legislación o fijados por otra autoridad.

Eficiencia: Está referida a la relación existente entre los bienes o servicios producidos o entregados y los recursos utilizados para ese fin, en comparación con un estándar de desempeño establecido.

Efecto: Constituye el resultado adverso o potencial que resulta de la condición encontrada. Generalmente, representa la pérdida en términos monetarios originada por el incumplimiento en

el logro de la meta. La identificación del efecto es un factor importante al auditor, por cuanto le permite persuadir a la gerencia acerca de la necesidad de adoptar una acción correctiva oportuna para alcanzar el criterio o la meta.

Estructura de control interno: Es el conjunto de planes, métodos, procedimientos y otras medidas, incluyendo la actitud de la dirección de una entidad, para ofrecer seguridad razonable respecto a que están lográndose los objetivos del control interno.

Estructura organizacional: Proporciona el marco dentro de la cual se planean, ejecutan, controlan y supervisan sus actividades, a fin de lograr los objetivos u metas establecidos.

Ética: Está conformada por valores morales que permiten a la persona adoptar decisiones y tener un comportamiento correcto en las actividades que le corresponde cumplir en la entidad.

Hallazgo de auditoria: Este concepto es utilizado para describir el resultado de la comparación que se realiza entre un criterio y la situación actual encontrada durante el examen a una área, actividad u operación o circunstancias en las cuales el criterio fue aplicado. Un hallazgo de auditoria representa algo que el auditor ha encontrado durante su examen y comprende una reunión lógica de datos, así como la presentación objetiva de los hechos y otra información pertinente. Es toda información que a juicio del auditor, permite identificar hechos o circunstancias importantes que inciden en forma significativa en la gestión de la entidad auditada, tales como debilidades o deficiencias en los controles gerenciales o financieros y que, por lo tanto, merecen ser comunicados en el informe; siendo sus elementos: condición, criterio, causa y efecto.

Integridad: Constituye una calidad de la persona que mantiene principios morales sólidos y vive en un marco de valores.

Monitoreo: Representa al proceso que evalúa la calidad del control interno en el tiempo y permite al sistema reaccionar en forma dinámica, cambiando cuando las circunstancias así lo requieran. Se orienta a la identificación de controles débiles, insuficientes o innecesarios y, promueve su reforzamiento. El monitoreo se lleva a cabo de tres formas:

a) Durante la realización de actividades diarias en los distintos niveles de la entidad

b) De manera separada por personal que no es el responsable directo de la ejecución de las actividades, incluidas las de control.
c) Mediante la combinación de ambas modalidades.

Observación: Esta referida a hechos o circunstancias significativos identificados durante el examen que pueden motivar oportunidades de mejoras. Si bien el resultado obtenido adquiere la denominación de hallazgo, para fines de presentación en el informe se convierte en observación.

Papeles de trabajo: Documentos que contienen la evidencia que respalda los hallazgos, observaciones, opiniones de funcionarios responsables de la entidad examinada, conclusiones y recomendaciones del auditor. Deben incluir toda la evidencia que se haya obtenido durante la auditoria.

Planeamiento: Fase de la auditoria durante la cual el auditor se aboca a la identificación de que examinar, como, cuando y con que recursos, así como la determinación del enfoque de la auditoria, objetivos, criterios y estrategia.

Plan de revisión estratégica: Acciones limitadas de evaluación, durante la fase Planeamiento, tendientes a determinar el alcance del examen así como su auditabilidad.

Plan de Auditoria: Tiene por propósito definir el alcance global de la auditoria de gestión, en términos de objetivos generales y objetivos específicos por áreas que serán materia de examen. Este documento incluye:

- Origen de la acción
- Objetivos de la auditoria
- Alcance de la auditoria, especificando períodos
- Áreas que serán examinadas, incluye objetivos específicos y alcance
- Criterios de auditoria a utilizarse
- Recursos de personal y especialistas que se necesitan
- Información administrativa

    - Presupuesto de tiempo
    - Informes a emitir y fechas de entrega

- Formato tentativo del informe.

Política: Se define como la declaración general que guía el pensamiento durante la toma de decisiones. La política es una línea de conducta predeterminada que se aplica en una entidad para llevar a cabo todas las actividades, incluyendo aquellas no previstas.

Políticas de administración de recursos humanos: Se relacionan con la contratación, orientación, capacitación, evaluación, asesoría, promoción, remuneración del personal de la entidad.

Procedimientos operativos: Son los métodos utilizados por el personal de la entidad para efectuar las actividades de acuerdo con las políticas establecidas. También son series cronológicas de acciones requeridas, guías para la acción que detallan la forma exacta en que deben realizarse ciertas actividades.

Programa de auditoria: Documento, preparado por el auditor encargado y el supervisor encargado, donde se señala las tareas específicas que deben ser cumplidas por el equipo de auditoria para llevar a cabo el examen, así como los responsables de su ejecución y los plazos fijados para cada actividad.

Procedimientos de auditoria: Son operaciones específicas que se aplican en una auditoria e incluyen técnicas y prácticas que son considerados necesarios en las circunstancias.

Recomendaciones: Constituyen las medidas sugeridas por el auditor a la administración de la entidad examinada para la superación de las observaciones identificadas. Deben estar dirigidas a los funcionarios que tengan competencia para disponer su adopción y estar encaminadas a superar la condición y las causas de los problemas.

Responsabilidad (traducción del inglés accountability): Se entiende como el deber de los funcionarios o empleados de rendir cuenta ante una autoridad superior y, ante el público, por los fondos o bienes del Estado a su cargo y/o por una misión u objetivo asignado y aceptado.

Revisión estratégica: Tiene como objetivo explorar en forma efectiva y eficiente las áreas de trabajo de auditoria establecidas durante la etapa de revisión general y profundizar el conocimiento inicial de los asuntos más importantes.

Síntesis: Tiene como objetivo hacer que el informe sea de mayor utilidad para los usuarios. Como de los receptores de los informes sólo leerán la síntesis, es importante que ésta refleje el contenido del informe de manera clara y precisa. La síntesis debe presentar en forma exacta, clara y justa los aspectos más importantes del informe, a fin de evitar errores de interpretación.

Sistema de información contable: Está constituido por los métodos y procedimientos establecidos para registrar, procesar, resumir e informar sobre las operaciones financieras de una entidad. La calidad de la información que brinda el sistema afecta la capacidad de la gerencia para adoptar decisiones adecuadas que permitan controlar las actividades de la entidad.

Sistema de Información Computarizada (SIC): Parte de un sistema general de información que emplea el equipo, los métodos y los procedimientos necesarios para procesar la información por medios electrónicos.

Sistema: Cualquier conjunto cohesionado de elementos que están dinámicamente relacionados para lograr un propósito determinado.

Técnicas de auditoría: Son métodos prácticos de investigación y prueba que utiliza el auditor para obtener evidencia necesaria que fundamente su opinión.

TERMINOS DE SEGURIDAD INFORMATICA

Acceso (access): Un sujeto o capacidad del objeto para usar, manipular, modificar, o afectar a otro sujeto o el objeto es referido como un acceso. Usuarios autorizados tienen acceso legal a un sistema, mientras que los hackers tienen un acceso ilegal a un sistema.

Activo (asset): Es un recurso de la organización que esta siendo protegido. Un activo podría ser lógico, así como un sitio en Internet, información o datos, o un activo puede ser físico así como una persona, una computadora personal, o cualquier otro objeto tangible.

Ataque (attack): Es un acto que es intencional o sin intención que atenta a causar daño ó comprometer la información y/o los sistemas que soporta.

Control, Salvaguardar, contramedidas: Estos términos representan mecanismos de seguridad, políticas, o procedimientos que pueden exitosamente contrarrestar ataques o reducir el riesgo, resuelve vulnerabilidades, mientras se improvisa la seguridad dentro de una organización.

Intrusión (Exploit): Hay dos formas comunes de esta palabra en términos de seguridad, primero los hackers pueden atentar una intrusión a un sistema o información usándolo ilegalmente por su personal. Segundo, una intrusión puede ser un blanco de una solución para un uso inadecuado por un agujero ó vulnerabilidad específica, usualmente es un software, que un hacker puede formular para un ataque. Esta es una forma de tomar ventaja de una vulnerabilidad ya conocida o una debilidad.

Exposición: La exposición de un sistema de información es un caso simple cuando el sistema es abierto para dañar. Las vulnerabilidades pueden causar exposición para daños potenciales o ataques de amenazas. La total exposición es el grado en el cual los activos de la organización están en riesgo de un ataque por parte de una amenaza.

Hacking: Puede ser definido positivamente o negativamente “escribir programas para diversión, Ganar acceso a una computadora ilegalmente”. Al principio de la computación fueron llamados Hacks, o hackers aquellos que podían romper los códigos de computación o manipular sus salidas. Es otra manera de hacer tecnología computacional, actualmente esta actividad es ilegal.

Objeto: Es una entidad pasiva en los sistemas de información que recibe o contiene información. Los objetos son asignados a específicos controles que restringen o previenen accesos no autorizados. Ejemplo, Impresores, Servidores, Bases de datos, o cualquier otro recurso compartido.

Riesgo (risk): Es la probabilidad que algo puede suceder. En seguridad de la información, podría ser la probabilidad de una amenaza a un sistema, la probabilidad de una vulnerabilidad siendo descubierta, o la probabilidad de un equipo o software no funcione correctamente. El riesgo puede ser medido en cantidades es decir en porcentajes o cualitativamente ejemplo "Una baja probabilidad de malfuncionamiento".

Modelo de la seguridad (security Blueprint): Es el plan para la implementación de nuevas medidas de seguridad en la organización. Algunas veces es llamado marco de trabajo (framework). El modelo de seguridad representa un cercamiento organizado a la planeación de los procesos de seguridad.

Modelo de la Seguridad (model security): Es una colección de reglas específicas de seguridad que representa la implementación de una política de seguridad.

Postura de Seguridad o Perfil de Seguridad: Este se refiere a la implementación de seguridad en una organización. Es en general una viñeta para la combinación de todos, políticas, procedimientos, tecnología, y programas que hacen el total esfuerzo de seguridad. Algunas veces es llamado Programa de Seguridad de la información.

Sujeto (subject): Es una entidad activa que interactúa con un sistema de información y causa que la información se mueva a través de los sistemas para un fin específico. Un sujeto puede ser individual, componente técnico, o procesos de computadoras, usuarios, servidores, etc.

Amenazas (threats): Es una categoría de objeto, persona u otra entidad que represente un peligro potencial a un activo.

Agente de Amenaza (Threat agent): Es una instancia específica o componente de una amenaza. Por ejemplo, se podría pensar acerca de todos los hackers en el mundo como una colección de amenazas.

Vulnerabilidad: Son debilidades o fallas en un sistema o mecanismo de protección que expone la información para atacarla o dañarla. Estos pueden variar desde un defecto (flaw) en una paquetería de software, a un desprotegido puerto de un sistema, o una puerta abierta.

ANEXO E

PLAN DE PUESTA EN MARCHA

Generalidades:

El presente material es una guía de uso para llevar a cabo el proceso de implantación del software de control de auditoría ISO17799, en este se describen las diferentes actividades que es necesario desarrollar para el buen funcionamiento del sistema, el orden de las actividades, el personal responsable y los tiempos estimados para cada actividad. A continuación se presenta a detalle este plan de implantación.

Requisitos previos:

a) Equipo de cómputo (Hardware). Es necesario contar con el equipo descrito en la sección de factibilidad técnica. Tener listo un servidor que funcione como servidor Web, otro como servidor de base de datos; auque podría ser un solo servidor a cargo de estas dos funciones.

b) Software: El sistema esta diseñado para trabajar sobre ambiente Windows o Linux; por lo que se requiere del siguiente software:

- Sistema Operativo: Windows o Linux versión de servidor
- Servidor Web: Apache o IIS (Internet Information Server)
- Modulo PHP: PHP 5 o versión actualizada, para el sistema operativo seleccionado
- Motor de base de datos: Mysql , instalador para el sistema operativo seleccionado

Para el caso del software de código abierto puede descargarse gratuitamente de los siguientes sitios:

Linux: http://www.linuxiso.org/

PHP: http://www.php.net/downloads.php

Mysql: http://dev.mysql.com/downloads/

Apache: http://httpd.apache.org/download.cgi

Para el caso de Microsoft es necesario tener licencia del Sistema Operativo Windows y del Servidor Web IIS (Internet Information Server), ver más información en: http://www.microsoft.com/downloads/search.aspx?displaylang=es

c) Información Inicial en el Sistema:

El código fuente del Sistema y la base de datos inicial viene con información básica para su funcionamiento, los catálogos que vienen con información lista para ser utilizada son:

- Roles
- Base de conocimiento de la norma ISO 17799
- Acción
- Reglas de decisión
- Paramentos del informe
- Referencias

Nota: Los catálogos Acción, Reglas de decisión, Referencia es necesario realizar una actividad de preparación y actualización para que se han específicos para las necesidades de la organización. Además la copia inicial del sistema viene con un usuario administrador admin y clave: admin, el cual permitirá hacer uso del sistema la primera vez; pero se recomienda su eliminación posterior por efectos de seguridad.

c) Estudio y definición de reglas de decisión del sistema:

El sistema permite la administración de las reglas de decisión, las cuales tienen la responsabilidad de determinar el nivel de conformidad con la norma ISO 17799, además ofrecer las recomendaciones necesarias las cuales permitan posibilidades de mejoras. Por tal razón la organización tiene la responsabilidad de desarrollar un estudio y análisis para la definición de sus reglas acorde a sus necesidades particulares, que luego son actualizadas en el sistema y que serán parte del motor de decisión.

Equipo de trabajo:

El grupo de trabajo deberá ser establecido en conjunto por la Unidad de Administración académica, y tecnología y Comunicaciones, y debe incluir el siguiente personal.

- Un persona de la función de mantenimiento y operación
- Un Administrador de Sistemas con conocimientos de entornos Web(Web Master)
- Una persona para recibir el entrenamiento del uso del software, y recibir el conocimiento necesario para la función de administrador del sistema.

Funciones del grupo de trabajo.

Las funciones del grupo de trabajo están directamente relacionadas con la instalación, configuración, integración, prueba y certificación del buen funcionamiento del sistema.

Actividades:

Los principales elementos del proceso de implantación se resumen en los siguientes pasos:

- Instalación del Sistema Operativo (Windows o Linux)
- Instalación del Servidor Web (Web Server)
- Prueba de instalación del Servidor Web
- Configuración y optimización del Servidor Web (http.conf)
- Instalación del modulo de PHP
- Configuración y optimización de PHP (php.ini)
- Integración de PHP con el Servidor Web
- Prueba de funcionamiento de paginas Web utilizando PHP
- Instalación de motor de base de datos Mysql
- Prueba de conexión con motor de base de datos
- Ejecución de Script de creación de base de datos del sistema
- Revisión y prueba de creación de la base de datos del sistema
- Creación de sitio dentro del Servidor Web
- Incorporación de código fuente del sistema

- Configuración de permisos a nivel de Servidor Web para acceder el sistema
- Pruebas de conexión con el sistema
- Prueba de uso del sistema
- Prueba de rendimiento del sistema
- Creación de cuentas de usuario (Administrador, Evaluador, Ejecutivo y Consulta)
- Prueba de correcto funcionamiento de cuentas de usuario creadas
- Adición de unidades a ser parte del catalogo de departamento del sistema
- Actualización de reglas de decisión
- Capacitación del sistema
- Finalización del proceso de Implantación

Nota: Para apoyo técnico referirse al manual de instalación del sistema

Cronograma de Actividades:

No.	Actividad	Duración	Responsable
1	Instalación Sistema Operativo	2.0 Hrs.	Web Master
2	Instalación de Web Server	1.0 Hr.	Web Master
3	Prueba de Instalación	0.5 Hr.	Técnico de Operaciones
4	Configuración de Web Server	1.0 Hr.	Web Master
5	Instalación de Modulo PHP	0.5 Hr.	Web Master
6	Configuración de PHP	0.5 Hr.	Web Master
7	Integración de PHP con Servidor Web	0.5 Hr.	Web Master
8	Prueba de funcionamiento de paginas dinámicas y estáticas(.php y .html)	0.5 Hr.	Web Master
9	Instalación de motor de base de datos	0.5 Hr.	Web Master
10	Prueba de conexión con motor de BD	0.5 Hr.	Web Master
11	Ejecución de Script de creación de BD del sistema	0.5 Hr.	Web Master
12	Prueba y revisión de consultas con la BD del sistema	1.0 Hr.	Web Master

13	Creación de sitio web	0.5 Hr.	Web Master
14	Incorporación de código fuente del sistema	0.5 Hr.	Web Master
15	Configuración de seguridad del sitio a nivel del Servidor Web	1.0 Hr.	Web Master
16	Prueba de conexión con el sistema	0.5 Hr.	Técnico de Operaciones
17	Prueba de funcionamiento del sistema	2.0 Hrs.	Técnico de Operaciones
18	Prueba de rendimiento del sistema	2.0 Hrs.	Técnico de Operaciones, Web Master
19	Creación de cuentas de usuario	1 Hr	Administrador del Sistema ISO17799
20	Pruebas de correcto funcionamiento de cuentas de usuario	1 Hr	Administrador del Sistema ISO17799
21	Adición de unidades a ser parte del sistema en catalogo de departamentos	1 Hr	Administrador del Sistema ISO17799
22	Actualización de reglas de decisión	10 Hrs.	Administrador del Sistema ISO17799
23	Capacitación del uso del sistema	8.0 Hrs.	Administrador del Sistema ISO17799
24	Certificación y finalización del proceso de implantación	1 Hr.	Web Master, Técnico de Operaciones y Jefe de unidades de Administración Académica y Tecnología y comunicaciones.
25	Imprevistos	2.5 Hrs	
	Total de Horas:	**40 Hrs.**	

ANEXO F

DISEÑO DE HERRAMIENTA DE INVESTIGACION