SISTEMAS DE INFORMACIÓN EN LABORATORIOS DE INVESTIGACIÓN EN BIOMEDICINA: AUDITORÍA INFORMÁTICA PRELIMINAR BASADA EN COBIT

Òscar Coltell[*,1,3], Ricardo Chalmeta[1], Dolores Corella[1,3], José M. Ordovás[3].*
1:Grupo de investigación en Integración y Re-Ingeniería de Sistemas (IRIS).
Departamento de Lenguajes y Sistemas Informáticos.
Universitat Jaume I. Castellón.
2: Unidad de Epidemiología y Genética Molecular.
Departamento de Medicina Preventiva y Salud Pública.
Univesitat de València, Valencia.
3: Nutrition and Genetics Laboratory, Human Nutrition Research
Center on Aging, Tufts University, Boston (USA)

INTRODUCCIÓN

La investigación en Biomedicina en la actualidad exige la concurrencia de recursos humanos y tecnológicos específicos [8] [9]. La formación de los recursos humanos y la complejidad y sofisticación del resto hace que los presupuestos manejados por los laboratorios de investigación sean muy altos [10] y lo problemas muy diversos [2] [7]. Sin embargo, los instrumentos de control y optimización de dichos recursos no están muy desarrollados en este campo [7].

Por lo tanto, el objetivo del trabajo que se presenta ha sido la realización de una auditoría de sistemas de información en un laboratorio de investigación biomédica para obtener el diseño de un instrumento de control en la organización y aplicación de los sistemas informáticos como soporte de los procesos científicos.

MATERIAL Y MÉTODOS

Se ha empleado fundamentalmente el marco metodológico de auditoría de sistemas de información COBIT (*Control Objectives for Information Technology*) [4] de la *Information Systems Audit and Control Asociación* (ISACA, http://www.isaca.org). También se han aplicado los principios y las normas de trabajo de la Auditoría Informática [1][6]. Por otra parte, se han estudiado las características particulares de un laboratorio de investigación en Biomedicina, las necesidades de soporte informático, la estructura organizativa interna y las dependencias externas con relación a la institución en la que se halla. La unidad organizativa tomada como referencia es el *Nutrition and Genomics Laboratory, JM-USDA Human Nutrition Research Center on Aging at Tufts University*, Boston, MA, EE. UU.

El modelo de auditoría bioinformática

Se plantea un modelo de desarrollo de auditoría para la Función Bioinformática basado en el COBIT [4] [5] que está ampliamente descrito en [3]. Dicho modelo consiste en la definición de las subfunciones principales de la Bioinformática: Investigación Teórica, Gestión de la Investigación, Aplicación de la Investigación, Desarrollo Tecnológico, Formación y Seguridad y Protección de la Información.

Descripción y estructura organizativa del objeto de estudio

El *Nutrition and Genomics Laboratory*, perteneciente al *JM-USDA Human Nutrition Research Center on Aging at Tufts University*, Boston, MA, EE. UU., es un laboratorio de investigación creado en 2000 por su responsable, el Dr. José M. Ordovás, que surge del más antiguo *Lipid Metabolism Laboratory*, encuadrado en el mismo centro. El *Human Nutrition Research Center* es un instituto de investigación cofinanciado por el Departamento de Agricultura de los EE. UU. (USDA), y la Universidad *Tufts*.

Las actividades de investigación realizadas por este laboratorio combinan la alta investigación en Epidemiología Genética, Nutrición Genómica (Nutrigenómica), Metabolómica y Transcriptómica. En la Epidemiología Genética se trabaja sobre las asociaciones genotipo-fenotipo y las interacciones gen-dieta. En la Nutrigenómica se trabaja sobre estudios de intervención dietaria. En la Metabolómica se trabaja sobre los biomarcadores no invasivos del envejecimiento saludable. Y finalmente, en la Transcriptómica se trabaja sobre los mecanismos de la respuesta dietaria y nuevos genes relacionados con los procesos de envejecimiento. La estructura orgánica estable del laboratorio se muestra en la Tabla 1. Por cuestiones de confidencialidad, no se incluyen los nombres propios de los miembros del laboratorio excepto la de su responsable.

Miembro	Perfil	Asignación	Puesto
J. M. Ordovás	Director	Despacho de investigación	Staff
Miembro Nº 02	Genetista	Despacho de investigación y laboratorio	Staff
Miembro Nº 03	Técnico de laboratorio	Laboratorio	Staff
Miembro Nº 04	Técnico de laboratorio	Laboratorio	Staff
Miembro Nº 05	Técnico de investigación	Despacho de investigación y laboratorio	Estudiante predoctoral
Miembro Nº 06	Técnico de investigación	Despacho de investigación y laboratorio	Estudiante predoctoral
Miembro Nº 07	Técnico de investigación	Despacho de investigación y laboratorio	Estudiante
Miembro Nº 08	Graduate Student	Despacho de investigación y laboratorio	Estudiante
Miembro Nº 09	Graduate Student	Despacho de investigación y laboratorio	Estudiante

Además, se produce durante el año una rotación de investigadores procedentes del extranjero, en calidad de científicos visitantes o de becarios postdoctorales. Esta afluencia de visitas ha dado lugar a que el laboratorio mantenga una gran cantidad de colaboraciones con los investigadores que han estado allí y con sus respectivos centros. En la Figura 1 se muestra la arquitectura funcional y de responsabilidades del laboratorio, donde se destacan los instrumentos principales.

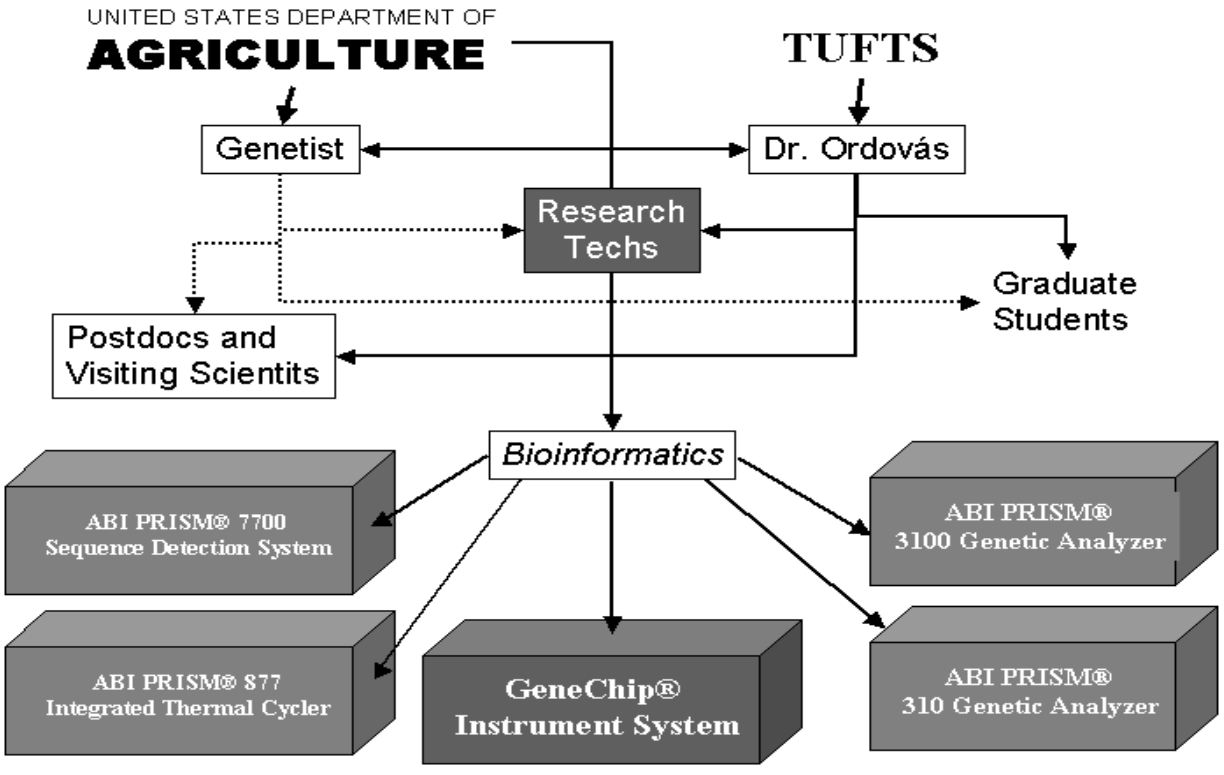

Figura 1. Arquitectura funcional y de responsabilidades del laboratorio

Como se puede observar, la dirección y supervisión de los técnicos de laboratorio, los estudiantes y los científicos visitantes, está compartido entre el director del laboratorio y el genetista. Por otra parte, se muestra una Función Bioinformática que tiene a su cargo el control de la instrumentación principal y que también depende del director y del genetista. Esta función no está cubierta por ningún personal en la actualidad. El laboratorio como unidad orgánica dispone de dos laboratorios de investigación biomédica y molecular que contienen esta instrumentación principal y otros instrumentos y elementos auxiliares habituales en este tipo de laboratorios. En la actualidad tampoco no existe personal auxiliar asignado para desempeñar funciones de administración general y económica de las operaciones diarias del laboratorio.

La estructura de sistemas informáticos del laboratorio se muestra en la Tabla 2. Cabe destacar que casi todos los integrantes del mismo tienen un equipo informático asignado para llevar a cabo trabajos generales, redacción de documentos científicos, búsqueda de bibliografía por Internet e intranet, comunicación a través de correo electrónico y otras tareas ofimáticas auxiliares. La excepción son los dos técnicos de laboratorio, que actualmente comparten el mismo equipo, puesto que uno de ellos se ha incorporado recientemente, y un *graduate student* que solamente utiliza uno de los laboratorios para los experimentos que determinan los supervisores.

Tabla 2. Estructura de sistemas informáticos del Nutrition and Genomics Laboratory

Equipo	Sistema Operativo	Lugar de asignación	Responsable
PC, DELL, P-III	Windows 2000 Pro.	Despacho de investigación director	J. M. Ordovás
PC, Gateway, P-II	Windows 2000 Pro.	Despacho de investigación director	J. M. Ordovás
Laptop, Sony, P-III	Windows XP HE	Despacho de investigación y exterior	J. M. Ordovás
Laptop, Toshiba, P-III	Windows 2000 Pro.	Despacho de investigación staff y exterior	Genetista
PC, Apple, Imac	Apple MacOS 9.0	Laboratorio	Técnico de laboratorio
PC, DELL, P-III	Windows 2000 Pro.	Despacho de investigación staff	Técnico de investigación
PC, DELL, P-III	Windows 2000 Pro.	Despacho de investigación estudiantes	Técnico de investigación
PC, DELL, P-III	Windows 2000 Pro.	Despacho de investigación estudiantes	Técnico de investigación
PC, Gateway, P-II	Windows 98 SE	Despacho de investigación estudiantes	Graduate Student
PC, DELL, P-III	Windows NT 4.0.	Laboratorio. ABI PRISM® 7700 Sequence Detection System	Técnico de laboratorio
PC, DELL, P-II	Windows NT 4.0.	Laboratorio. ABI PRISM® 3100 Genetic Analyzer	Técnico de laboratorio
PC, DELL, P-II	Windows 98	Laboratorio. ABI PRISM® 310 Genetic Analyzer	Técnico de laboratorio
PC, Apple	Apple MacOS 8.0	Laboratorio. ABI PRISM® 877 Integrated Thermal Cycler	Técnico de laboratorio
HP 4500 Laserjet	Postscript	Salita común	Técnico de laboratorio

El laboratorio no dispone de personal técnico informático propio sino que está asistido por personal del Departamento de Computación del centro. Dicho departamento dispone de dos técnicos para dar servicio a un edificio de catorce plantas, incluyendo el parque de ordenadores y la red local del edificio. No se ha facilitado datos sobre el parque de ordenadores del centro.

El proyecto de auditoría: planteamiento

El *contexto del problema* es la aplicación de una auditoría de sistemas de información a un laboratorio de investigación en Biomedicina que ha incorporado la Función Bioinformática como una función principal en sus actividades [3]. El *alcance del estudio* consiste en la auditoría sobre la Función Bioinformática en las áreas de organización, metodologías y técnicas de ingeniería, tecnologías y políticas e instrumentos de investigación y gestión. Por lo tanto, el *objetivo de la auditoría* es la realización de un proyecto de auditoría preliminar sobre la Función Bioinformática como soporte de la investigación biomédica en un laboratorio de investigación en el mismo campo. En la Figura 2 se muestran las fases de un proyecto completo de auditoría [1] [6]. Se ha hecho la distinción entre dos rutas, la ruta 1 y la ruta 2. La ruta 1 corresponde a una auditoría preliminar ya que no aplica dos fases importantes de pruebas y las pruebas realizadas no lo son en profundidad. En cambio, la ruta 2 corresponde a una auditoría ordinaria.

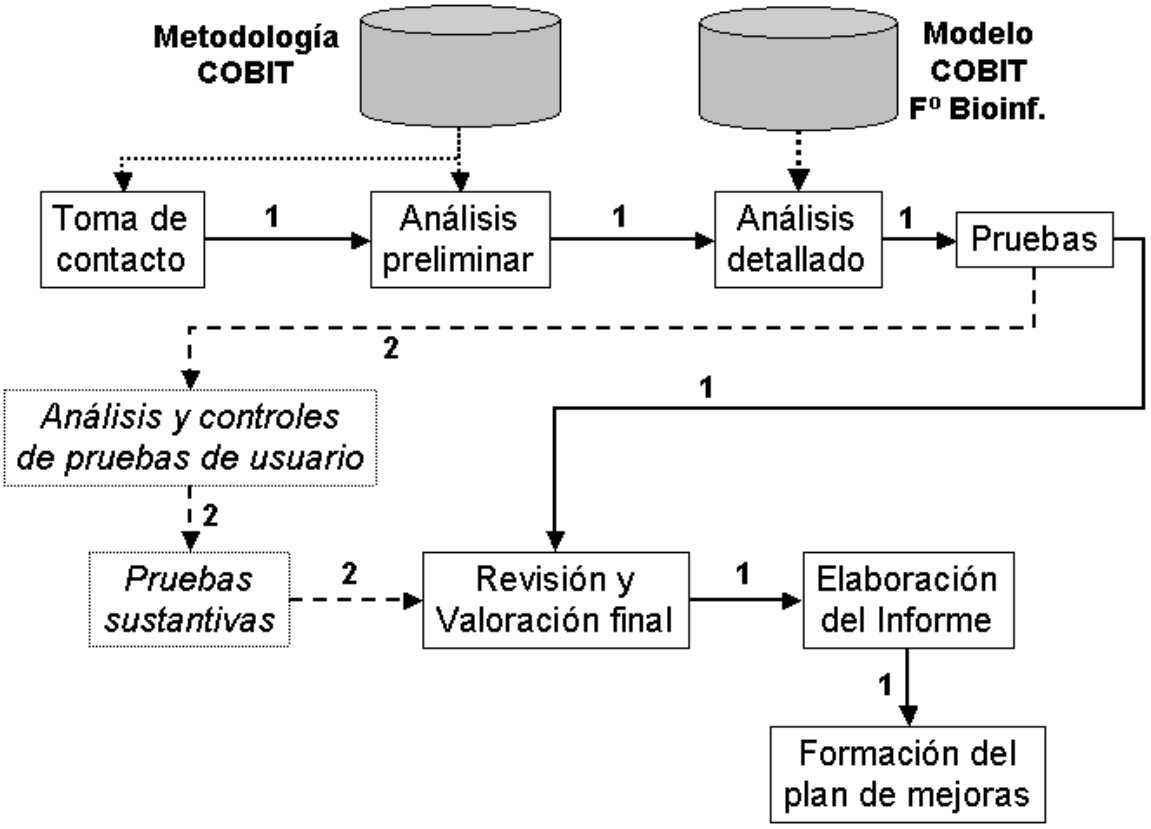

Figura 2. Fases de un proyecto de auditoría

El marco metodológico que se aplica inicialmente es el COBIT [4]. Sin embargo, para el proyecto en particular, se ha previsto aplicar el modelo de COBIT adaptado para la Función Informática [3]. Concretamente, se pretende aplicar la Guía de Auditoría de la Función Bioinformática. La Guía de Auditoría de la Función Bioinformática tiene asociado un juego de cuestionarios que se diseñaron y elaboraron en un proyecto académico de la titulación de Ingeniería Informática dirigido por O. Coltell (véase la sección de agradecimientos).

RESULTADOS

Se ha realizado un proyecto de auditoría de sistemas de información con las siguientes características: grado preliminar; alcance restringido a la aplicación de sistemas informáticos como soporte a los procesos científicos y a la organización de los recursos; el ámbito es el laboratorio tomado como una unidad organizativa casi independiente donde se plantean problemas comunes a las empresas y administraciones, pero también se añaden otros relativos a los procedimientos científicos. Se ha realizado una guía de auditoría específica para este ámbito adaptando la Guía de Auditoría de la Función Bioinformática [3]. En esta sección solamente se describirán los resultados más destacables.

Resultados del Análisis

Una vez realizado el análisis se han identificado determinados riesgos relativos a la estructura orgánica del laboratorio actual (Figura 1), a la seguridad física y a la operatividad y mantenibilidad de los equipos. A continuación, se describen con más detalle estos resultados.

Riesgos relativos a la estructura orgánica

La estructura bicéfala que existe actualmente puede dar lugar a colisión de flujos de órdenes y de información hacia los técnicos de laboratorio, y los técnicos de investigación. El director del laboratorio tiene una fuerte carga de trabajo científico y docente. Además, suele ausentarse con frecuencia para cumplir con diversos compromisos científicos en todo el mundo.

Riesgos relativos a la seguridad física

El servicio de seguridad del centro no es completo ya que faltan o no funcionan elementos de vigilancia activa. Esta situación pone en riesgo físico determinados equipos que se encuentran en una salita de acceso libre que sirve además de distribuidor de los despachos. Actualmente, solamente se encuentra allí la impresora láser. Por otra parte, el acceso y el paso no es cómodo ya que todos los elementos mobiliarios han dejado un pasillo demasiado estrecho. Además, el propio funcionamiento de la impresora provoca un aumento de la contaminación acústica y térmica que puede llegar a interferir en el trabajo de quienes se encuentren en dicha salita.

Riesgos relativos a operatividad de los equipos

Se ha observado que uno de los equipos que está en el despacho del director, el PC Gateway P-II Windows 98 (Tabla 3), prácticamente está fuera de uso, pero se mantiene porque en su almacenamiento secundario se guarda información importante para el director. En el otro equipo, se ha observado que la cuenta de usuario habitual es la de Administrador, lo que comporta altos riesgos en cuanto a la seguridad lógica y a la configuración del equipo. La coexistencia física de los dos equipos dificulta la comodidad de trabajo. Además, puesto que el director maneja también un ordenador portátil, existe el riesgo de que no se tenga una idea clara de dónde está la información importante o de que esté duplicada.

Los equipos de los despachos de staff y estudiantes utilizan cuentas de *power user*, a excepción del equipo del genetista, que utiliza la cuenta de Administrador. En este caso, existen los mismos riesgos que con el equipo del director.

Los equipos de los laboratorios, a excepción del que está asignado a uno de los técnicos de laboratorio, son todos equipos supeditados al instrumental descrito en la Figura 1. Dichos equipos no se utilizan para tareas personales, con lo cual los riesgos son menores, pero están conectados a la red local para que se pueda acceder desde el resto de equipos.

Resultados de las Pruebas

Una vez realizadas algunas pruebas e inspecciones de los equipos, se han identificado determinados riesgos relativos a la seguridad lógica local y de red y a la fiabilidad de la información. A continuación, se describen con más detalle estos resultados.

Riesgos relativos a la seguridad lógica local

Una vez inspeccionados cada uno de los equipos se han podido detectar algunas anomalías de almacenamiento que comportan graves riesgos. Todos los equipos que tienen instalado el sistema operativo MS Windows 2000 disponen de un disco duro con una sola partición. Además, la mayoría de usuarios utilizan la carpeta "My documents" para guardar sus datos. Esto tiene el riesgo de la pérdida irreparable de la información si se procede a la reinstalación del sistema operativo o al formateo de la partición, y no se ha hecho copia de seguridad o ésta esté desactualizada. Por otra parte, no existe ninguna política de copias de seguridad y, en consecuencia, no se aplica ningún procedimiento para hacer copias periódicas del contenido de los equipos.

Riesgos relativos a la seguridad lógica de red

La utilización de cuentas de administrador en algunos equipos es un riesgo alto porque los privilegios de acceso que tienen permiten acceder a la red en general desde el exterior. Se ha observado que el Departamento de Computación ha instalado un programa de monitorización en cada uno de los equipos. Sin embargo, no se ha podido comprobar el grado de fiabilidad y no se ha recibido información sobre todas las funciones que realiza. Por otra parte, las cuentas de usuario de tipo *power user* dadas de alta en cada uno de los equipos tienen todas el mismo nombre, aunque distinta contraseña. Esto facilita el ataque por diccionario porque solamente se ha de obtener la contraseña.

Se ha comprobado también que los equipos no están asignados a un solo dominio de red, sino que algunos siguen con el dominio por defecto "WORKGROUP" y otros presentan diferencias de nombre. Esto hace que no sea fácil detectar cada uno de los equipos cuando se accede por medio de la red de Microsoft. Además, ninguno de los usuarios ha sido formado para utilizar con provecho las funciones de red a su alcance y así , por ejemplo, poder intercambiar información masiva. En tercer lugar, la ejecución de determinados programas en los equipos asignados al instrumental de laboratorio, está provocando riesgos de seguridad cuando se accede a dichos equipos desde los puestos de trabajo de los investigadores. Esto es porque dichos programas no incluyen mecanismos de seguridad o son demasiado antiguos.

Riesgos relativos a la fiabilidad de la información

Una detallada inspección de la estructura de ficheros de cada uno de los equipos ha detectado que ninguno de los usuarios está aplicando un procedimiento estandarizado y claro cuando guarda la información en su partición de disco. Incluso se han detectado carpetas de información dentro de los directorios correspondientes a la instalación de aplicaciones y al propio sistema operativo. Además, se ha observado que la mayor parte de la información se guarda en la carpeta "My documents" y no existe ninguna carpeta espejo en la cuenta de usuario, ni fuera de ella. No se puede saber así con claridad la información que está duplicada, obsoleta o se debe guardar off-line para despejar el disco duro.

El proyecto de auditoría se ha concluido con la elaboración de un informe final que contiene las recomendaciones de modificación y mejora de las condiciones, que están resumidas en la sección siguiente. No se ha elaborado el plan de mejoras puesto que es necesario definir previamente las responsabilidades de su ejecución entre el Laboratorio y el Departamento de Computación del HNRC.

DISCUSIÓN

Una de las conclusiones generales del estudio efectuado como proyecto de auditoría es que se pueden mejorar varios de los aspectos en que se han detectado altos riesgos, a corto y a medio plazo. A continuación se detallas dichas mejoras.

Mejoras en la organización

Es necesario definir con claridad todas las funciones realizadas por el Laboratorio y agruparlas a continuación en cinco grandes categorías: científicas, técnicas, administrativas, docentes y dirección y supervisión general. Seguidamente, se deben asignar las responsabilidades sobre dichas categorías. El director debe asumir directamente las funciones de dirección y supervisión general, delegando algunas de ellas en el genetista, en previsión de las ausencias por motivos profesionales.

Las funciones docentes deben estar asumidas por el director, aunque debe delegar algunas en los técnicos de investigación, que son estudiantes de doctorado. Las funciones científicas deben estar asumidas por el genetista y el director, pero asignando las no estratégicas al genetista de forma que, si el director no está disponible, no se produzcan retrasos o paros de la actividad del Laboratorio por falta de decisiones científicas.

Las funciones técnicas y administrativas deben asignarse al genetista para que ejerza su gestión y supervisión. Sin embargo, la ejecución de las mismas necesita de la incorporación de nuevo personal: un bioinformático y un administrativo. El bioinformático (puesto en proceso de provisión) debe asumir el control, supervisión y mantenimiento de los elementos que constituyen la Función Bioinformática. El administrativo debe llevar la administración general y económica del Laboratorio, descargando así al director y a los técnicos de laboratorio. El administrativo también puede hacerse cargo de las tareas de asistencia del director y del genetista: atención telefónica, gestión de la agenda, gestión de reservas para viajes, gestión de reservas de recursos del centro, filtro de visitantes puntuales, asistencia básica a los científicos visitantes, etc.

Con respecto a la arquitectura de sistemas informáticos, la mejor solución es la introducción de un servidor de red que controle directamente los equipos asociados al laboratorio y que actúe de firewall frente al acceso desde los equipos personales de los miembros del Laboratorio. Así, cualquier acceso a dichos equipos sería filtrado por el servidor que, por otra parte, daría servicio homogéneo y común a todos los investigadores. Este servidor podría tener la capa intermedia de servidor de aplicaciones y así centralizar las aplicaciones comunes de todo el Laboratorio. Además, dicho servidor podría servir como repositorio de la información común y particular de los miembro del Laboratorio y facilitar entonces la aplicación sistemática de un procedimiento de copias de seguridad y otro de mantenimiento remoto. La administración del servidor en una función asociada al bioinformático.

Los equipos deben ser revisados y sus discos particionados, para dejar una de las particiones dedicada a guardar solamente la información. Los usuarios deben tener una formación básica en el manejo de las estructuras de carpetas y ficheros y en el acceso a los recursos de red para que apliquen procedimientos de almacenamiento y salvaguarda estandarizados. Se debe revisar la configuración de red de cada equipo, para asignarles un único nombre de dominio. También se debería aplicar un procedimiento de asignación de nombres lógicos distinto del actual para facilitar el cambio de equipos y su identificación en el acceso remoto. Se debe revisar también el estado del sistema operativo y del hardware de cada equipo para optimizar su funcionamiento. Se debe acometer también la administración de cuentas, revisando las características de cada cuenta de usuario, diferenciando los nombres, y creando cuentas de usuario de tipo *power user* para el director y el genetista, y aplicando una política homogénea a las cuentas de administrador.

Conclusiones

El informe final del proyecto de auditoría ha permitido identificar los riesgos en la Función Bioinformática del *Nutrition and Genomics Laboratory* y ha servido para establecer los mecanismos de mejora. Por otra parte, este trabajo ha impulsado la revisión y adaptación de la Guía de Auditoría de la Función Bioinformática como la base de un proyecto de auditoría más exhaustivo que puede aplicarse a otros laboratorios de investigación, con cambios menores, para obtener los instrumentos de control necesarios en dicha función.

AGRADECIMIENTOS

Este trabajo ha sido financiado por el Ministerio de Educación y Ciencia de España, becas PR2002-0115 (D. Corella) y PR2002-0116 (O. Coltell), y parcialmente por CICYT (proyecto código DPI 2000-1058).

Algunos de los cuestionarios aplicados en el proyecto de auditoría proceden del Proyecto Informático de Ingeniería Informática realizado por José Manuel García Forner, recién licenciado en dicha titulación por la Universidad Jaume I (julio de 2002), y dirigido por uno de los autores, O. Coltell. Dicho proyecto se titula "Auditoría del Desarrollo de un Proyecto de Investigación: Elaboración de la Guía de Auditoría y Aplicación Práctica".

BIBLIOGRAFÍA

1. Benal R., Coltell O. Auditoría de los Sistemas de Información (reimpresión). Servicio de Publicaciones de la Universidad Politécnica de Valencia, Valencia, 1999.
2. Cass S., Riezenmann M.J. "Improving Security, Preserving Privacy". IEEE Spectrum, Jan.; 2002: 44-49.
3. Coltell O., Chalmeta R. "Auditoría Bioinformática". Actas del V Congreso Nacional de Informática y Salud, INFORSALUD 2002. Madrid, 2002.
4. ISACAF-B. COBIT. Framework. 3rd ed. ISACA, Rolling Meadows, IL (USA), 2000.
5. ISACAF-E. COBIT. Audit Guidelines. 3rd ed. ISACA, Rolling Meadows, IL (USA), 2000.
6. Piattini M., Del Peso E. (eds.) Auditoría Informática. Un enfoque práctico. Ra-Ma, Madrid, 1998.
7. Rindfleisch T.C. "Privacy, Information Technology, and Health Care". Communications of the ACM, 40-8; 1997: 93-100.
8. Rondel R. K., Varley S. A., Webb C. (eds.) Clinical Data Management. John Wiley, New York, 1993.
9. Sackman H. Biomedical Information Technology. Global Social Responsibilities for the Democratic Age. Academic Press, San Diego, CA (USA), 1997.
10. Van Bemmel J.H., Musen M.A.(eds.) Hadbook of Medical Informatics. Springer-Verlag, Heidelbeg, 1997.