Mejora al control de acceso para laboratorios

Víctor Méndez[1], Francisco Cruz[1],

[1] Escuela de Informática, Facultad de Ingeniería, Universidad Andrés Bello
República 239, Santiago, Chile
vmendezgallardo@gmail.com, fcruz@unab.cl

Resumen. El creciente aumento de la demanda del uso de laboratorios ha provocado que la minimización de los costos y tiempos requerida para realizar la mantención correctiva y preventiva de los recursos se vuelva una prioridad. La mejora consiste en varios subsistemas que se complementan para controlar el acceso a la información y uso de los computadores en clases, con el fin de disminuir el costo-tiempo requerido para las mantenciones y al mismo tiempo adaptarse a la normativa institucional vigente. Para este trabajo fue elegido la metodología IDEAL® de SEI, para la mejora continua de procesos, y la metodología DorCU para la elicitación de requerimientos. Esta mejora fue demostrada en una prueba de concepto con resultados satisfactorios.
Palabras claves: Control de acceso, seguridad informática, IDEAL, DoRCU

1 Introducción

En el área de informática y computación, el control de acceso, responde a la necesidad de regular la disponibilidad de información, recursos y servicios, los cuales sólo serán otorgados previa autorización de alguna entidad con la facultad de hacerlo. En otras palabras, se busca divulgar información, recursos y servicios pero de manera segura, no a todos quienes quieran acceder, sino que sólo a los que sean catalogados como entidades autorizadas. El modo de regular el acceso puede ser categorizado por la capacidad de leer o escribir información, ejecutar procesos en un dispositivo local o a través de la red, u otro criterio, donde cada una de estas capacidades está directa o indirectamente vinculada a los privilegios, vale decir, a la facultad de permitir o denegar dichas capacidades.
El control de acceso es un mecanismo que otorga confidencialidad e integridad a los sistemas, asegurando los recursos y controlándolos en base a un conjunto de políticas establecidas [1]. Esto permite especificar el acceso, otorgando tareas o grupos de tareas, a partir de privilegios que se establecen según el trabajo que deben realizar los usuarios [2], es decir, es utilizado como un mecanismo, método, herramienta o procedimiento para implementar políticas de control de acceso, que permita evaluar si una identidad establecida tiene autorización en base un contexto de seguridad existente y un recurso controlado. [3]
El control de acceso también es considerado como un proceso que busca regular mediante el uso de contraseñas, reconocimiento de direcciones Internet Protocol (IP) u otros medios similares, lo que requiere que el usuario sea autenticado y luego autorizado en base a permisos, de modo de limitar a quien obtiene y observa la información y bajo qué circunstancias [4], es decir, el control de acceso es sólo un aspecto de una solución de seguridad informática, pero es la más visible. Éstos se otorgan con el conocimiento de qué usuario puede acceder a un recurso específico, por lo tanto, se sabe quién puede hacer qué cosa y cuándo. [5]
Considerando la revisión anterior, es posible decir que el control de acceso es un proceso, que se basa en las políticas de seguridad informática vigentes en la institución, que busca regular el acceso a los recursos computacionales, asignando niveles de acceso, privilegios asociados y manejando información sobre quién usa qué recurso y bajo qué circunstancias.
El proyecto busca mejorar la situación actual de la Jefatura de Laboratorios (unidad a cargo de gestionar los recursos de los laboratorios de la Escuela de Informática de la Universidad Andrés Bello), en el ámbito del control de acceso a los equipos disponibles en los laboratorios, otorgando a dicha entidad mayor capacidad de mitigar y contener situaciones que puedan ocasionar problemas a los alumnos y profesores de la escuela, contribuyendo así al normal desempeño de sus usuarios y a la seguridad del entorno de trabajo en los laboratorios.
Mediante la recopilación de información a través de una encuesta (realizada a los alumnos y profesores de

la Escuela de Informática) y una reunión con el personal de laboratorios, se detectaron problemas relacionados con la conectividad de los equipos, modificaciones al sistema operativo o algún software en particular, ataques de virus, problemas en el hardware y en los procedimientos realizados para realizar el mantenimiento preventivo o correctivo, determinando que éstos ocurrían entre 2 a 4 veces por semana. Además, a pesar de que al inicio de cada semestre, los profesores solicitan software requerido para todo el período del semestre, existen circunstancias donde, por ejemplo, un profesor realiza la instalación de un software específico para una clase en particular sin autorización previa, o donde un alumno modifica un equipo sin ser autorizado, realizando cambios sin necesariamente cuidar que éste no afecte el normal desarrollo de las clases posteriores. Dichas situaciones ocurren por un inadecuado control de acceso o por la falta de éste, permitiendo al usuario realizar acciones que afecten la seguridad de la organización [6], por lo que el control de acceso es considerado como uno de los principales pilares en materia de seguridad informática, ya que a través de ésta se pueden mitigar las vulnerabilidades asociadas al usuario.

La propuesta consiste en una serie de sistemas complementarios, compuesto por procesos y procedimientos del personal, junto con políticas de seguridad implantadas en los equipos y controladas mediante un servidor. La idea es que el sistema resultante se fortalezca con las características de los subsistemas y entre éstos puedan aportar mayor control de los recursos que dispone la Jefatura de Laboratorios para uso académico.

Los resultados obtenidos fueron a partir de una prueba de concepto, donde se demostró que la propuesta permitía el normal desempeño de las asignaturas y al mismo tiempo cumplía con las políticas de seguridad de la institución.

2 Situación Actual

Para el año 2009 la Jefatura de Laboratorios cuenta con 7 laboratorios, cada uno equipado con alrededor de 30 equipos y otros dispositivos de red, como firewall, servidores, routers y switches, utilizados para uso académico, es decir, para realizar clases prácticas, de modo que el alumno pueda experimentar a partir de la teoría aprendida.

Hasta ese momento no existían procedimientos formales, vale decir que, dada la experiencia del personal, los procedimientos que realizan son en base a prácticas exitosas que han realizado anteriormente, pero que no necesariamente las comunican o las documentan debidamente. Entre las prácticas realizadas está el control de acceso de los laboratorios y equipos mediante solicitudes (fig. 1)

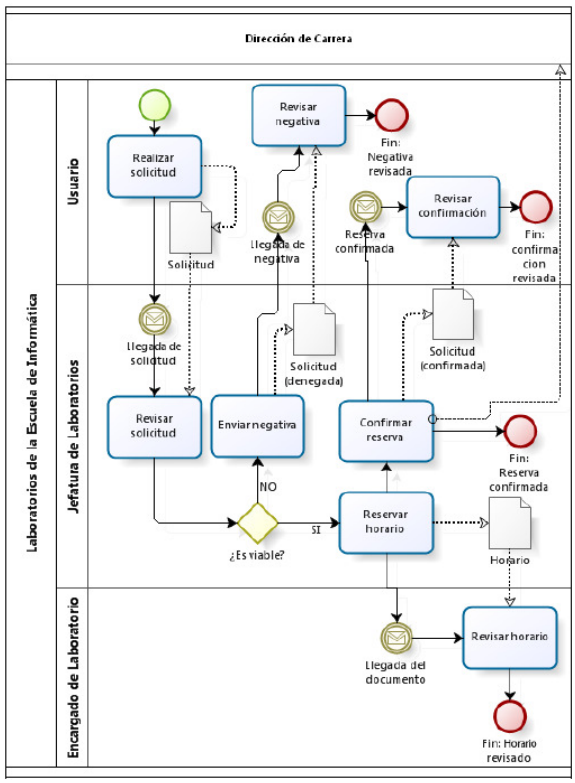

Fig 1: Proceso para reservar el uso del laboratorio. Modelado en base al estándar BPMN (Business Process Management Notation).

La figura 1 detalla la forma de controlar el acceso al laboratorio, que mediante el uso de un documento denominado "horario" se registra la reserva del recurso para todo el semestre, garantizando su disponibilidad a la asignatura que haya realizado dicho proceso. En caso de que se requiera para uso esporádico, se realiza un proceso de solicitud mediante el cual el Encargado de Laboratorios tomaba conocimiento de que el recurso ha sido requerido. Por otro lado, el acceso al equipo era controlado mediante el uso de perfiles de usuario, las cuales eran utilizadas de manera local e independientemente unos de otros, en otras palabras, en caso de requerir la modificación de alguna política de seguridad en el equipo, éste se debía realizar en cada uno de éstos.

Al recopilar la información obtenida desde diferentes perspectivas, se determinó que los problemas ocurridos en los laboratorios son por procedimientos internos, vale decir, la forma en que se realiza la

mantención correctiva y preventiva; a problemas con un software en particular; a la conectividad en los equipos; a los ataques de virus y problemas en el sistema operativo, los que en promedio ocurren 2 a 4 veces por semana (fig 2), provocando que los laboratorios no dispongan de los recursos requeridos para desarrollar una actividad programada al interior de éste. Junto con esto, se reveló que los usuarios resuelven sus problemas realizando principalmente cambios en el sistema operativo, modificando un software en particular o conectando su equipo personal, provocando que aquellas actividades programadas, dependientes de algún recurso en particular, resulten afectadas debido a la modificación realizada.

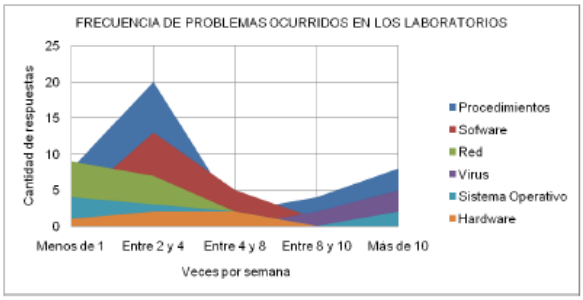

Fig 2: Frecuencia de los problemas detectados en los laboratorios.

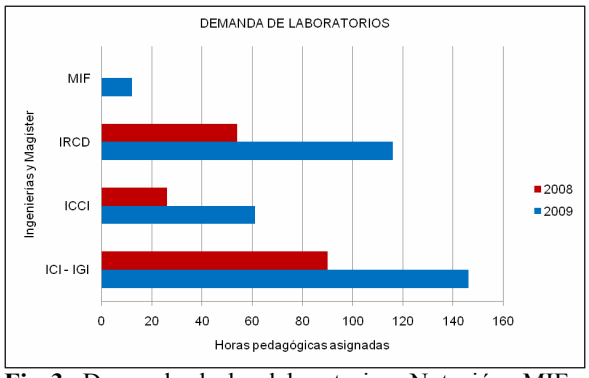

Fig 3: Demanda de los laboratorios. Notación: MIF (Magíster de Ingeniería Informática), IRCD (Ingeniería de Redes y Comunicación de datos), ICCI (Ingeniería Civil en Computación e Informática), ICI (Ingeniería en Computación e Informática), IGI (Ingeniería en Gestión Informática)

Además, cabe considerar que entre los objetivos y compromisos de la Escuela de Informática durante el 2008, está la elaboración de un plan para fidelizar al alumno mediante el aumento de clases prácticas en laboratorios [7], lo que conlleva a un crecimiento de más del 100% en la demanda del servicio que éstos ofrecen [8,9], por lo que la mitigación de cualquier imprevisto, que impida el normal desempeño de los usuarios, será primordial, ya que de ocurrir, el tiempo disponible no será suficiente para resolver el problema, considerando que durante la reunión del personal de laboratorios se determinó que, actualmente el tiempo requerido para resolver un inconveniente es entre 1 a 3 horas, según la complejidad del mismo. La figura 3 detalla la creciente demanda que reflejan los laboratorios, los periodos comparados son semestrales, vale decir, el 1er semestre del año 2008 con el primer semestre del año 2009.

3 Metodología

Para proponer una mejora a la situación descrita en la sección anterior, se llevaron a cabo actividades en base al modelo IDEAL (Iniciando, Diagnosticando, Estableciendo, Actuando, Aprendiendo), publicado por SEI (Instituto de Ingeniería de Software) para mejorar los procesos del software [10].

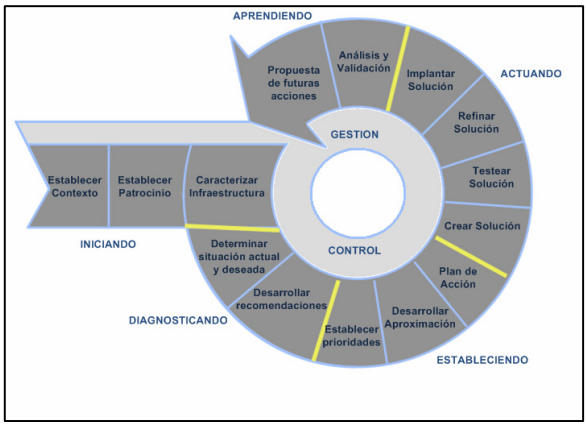

Fig 4: Metodología utilizada en el proyecto. Modelo IDEAL con una etapa transversal de gestión y control.

La figura 4 detalla las etapas de la metodología utilizada, donde la primera etapa se estableció el contexto del problema, procurando el apoyo de las entidades que están en la toma de decisiones y los recursos a requerir. Posteriormente en la segunda etapa se realizó el análisis de situación actual y realizando las recomendaciones pertinentes en base a las fortalezas y debilidades encontradas. En la tercera etapa se priorizaron los recursos y necesidades, planificando detalladamente las actividades a realizar. Durante la cuarta etapa, se procedió a realizar un estudio de requerimientos mediante la metodología DoRCU (Documentación de Requerimientos Centrada en el Usuario) [11], de modo que ambas

partes puedan conocer y comprender las necesidades documentadas. Luego de realizar dicho estudio se procedió con realizar la integración de los diferentes sistemas y probando sus funciones, para finalmente realizar una prueba de concepto. En la quinta etapa se realiza un análisis de los resultados obtenidos en la etapa anterior y se proponen futuras acciones para una segunda iteración. Transversalmente a las etapas descritas, se estableció una etapa de gestión y control, de modo que los cambios y riesgos puedan ser mitigados a tiempo y el proyecto pueda ser desarrollado como estuvo planificado originalmente.

4 Propuesta de mejora

La propuesta de mejora busca formalizar, estandarizar y establecer los principales pasos que deben realizar los funcionarios a cargo de los laboratorios de la Escuela de Informática, considerando las políticas y normativa informática vigentes [12]. Además, se establecen las responsabilidades de los respectivos cargos y roles, de modo de transparentar la labor de cada quién, aumentando consigo la seguridad de realizar correctamente los pasos necesarios para controlar el acceso a los equipos y a la información.
Los procedimientos que se estipularon, fueron segmentados en 2 secciones, procedimientos de acceso físico, que establece los diferentes pasos a seguir, frente a situaciones que involucre la autorización, configuración, reportes y solicitudes de acceso físico a los recursos existentes en los laboratorios; y por otro lado los procedimientos de acceso lógico, que busca estipular los pasos a seguir en circunstancias que requieran acceso o configuración de los recursos a nivel lógico. La propuesta para el control del acceso físico, en general fue promover la constante comunicación interna entre la jefatura y los encargados de laboratorios, haciendo uso del correo electrónico oficial (medio de comunicación formal en la institución) para publicar modificaciones en el horario, y por lo tanto tener actualizado el documento a nivel de toda la unidad. La figura 5 detalla uno de los procesos mejorados, la reserva del laboratorio para uso extra-programático, mecanismo mediante el cual se solicita un laboratorio para ser utilizado en actividades orientadas a promover las carreras de la Facultad de Ingeniería. Por otro lado, la propuesta para controlar el acceso lógico fue detallar el procedimiento con el cual se configuran los diferentes componentes del sistema, como por ejemplo la recuperación o desbloqueo de una cuenta de usuario perteneciente al dominio lógico de la unidad. La tabla 1 muestra en detalle los pasos que deben seguir los diferentes roles que participan en el procedimiento.

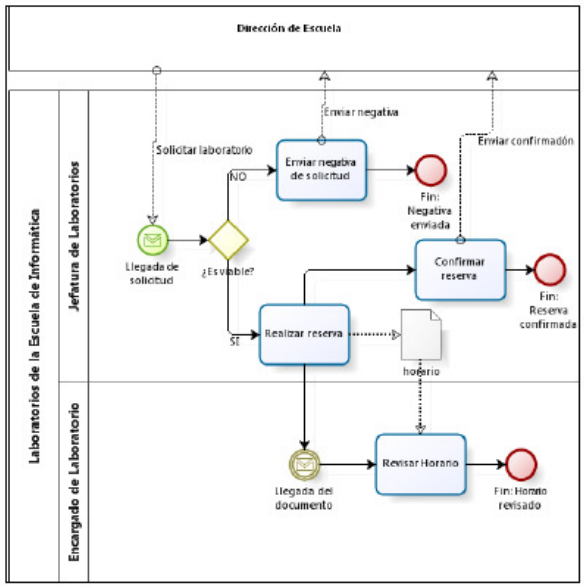

Fig 5: Proceso de reserva del laboratorio para uso extra-programático. Modelado en base al estándar BPMN (Business Process Management Notation).

Objetivo	Recuperar la contraseña o desbloquear la cuenta de usuario perteneciente al dominio
Responsable	**Descripción**
Usuario	Reporta olvido o bloqueo de su contraseña/cuenta de usuario
Jefatura de Laboratorios	Solicita al usuario identificarse mediante su credencial universitaria, carnet de identidad, pase escolar u otro documento que compruebe su pertenencia a la Facultad de Ingeniería o Escuela de Informática.
Usuario	Hace entrega de los documentos que identifican su pertenencia a la Facultad de Ingeniería o Escuela de Informática.
Jefatura de Laboratorios	Accede a la administración del dominio. Verifica la existencia de la cuenta de usuario bloqueada Establece la contraseña acorde a las políticas vigentes en la unidad. Notifica al usuario del procedimiento Realiza el reporte correspondiente Fin del procedimiento

Tabla 1: Procedimiento para recuperar/desbloquear la cuenta de usuario perteneciente al dominio de los laboratorios.

Una vez validados los procedimientos, se continuó con el establecimiento de políticas, de modo de buscar integrar los esfuerzos por controlar el recurso humano y tecnológico, junto con el conocimiento adquirido, regulando las responsabilidades y roles que son desempeñados en los laboratorios, con el propósito de mantener un ambiente coordinado y

comprometido tanto hacia los usuarios, como al personal de los laboratorios, de modo que puedan contribuir y actuar en base al documento. Las políticas que se propusieron se segmentan en dos secciones: control de acceso físico, que se basa en la regulación del acceso físico a determinados recursos disponibles en los laboratorios, tales como el cableado del equipo y el cableado de la red, con el propósito de establecer quién puede o no acceder a éstos, con tal de evitar eventuales problemas en la seguridad de los laboratorios; y control de acceso lógico, que busca regular el acceso a determinados recursos, como por ejemplo, las particiones del disco duro y las propiedades del sistema operativo, de modo que los usuarios puedan hacer uso de éstos y desempeñarse normalmente, sin involucrar a la seguridad de los laboratorios.

5 Resultados Obtenidos

Fueron realizadas una serie de pruebas para preparar el correcto funcionamiento del sistema, midiendo los tiempos que demora éste en estar listo para que el usuario pueda hacer uso del recurso. En la tabla 1 se detallan los tiempos que, en promedio, tardó el equipo en procesar algún evento, como por ejemplo: cuentas locales del sistema operativo o acceso a archivos compartidos en la red local. En dicha tabla, se puede apreciar que el mayor consumo de tiempo está en acceder al dominio, vale decir, en la prueba el servidor encargado de ejecutar las políticas implementadas, tardaba 15 minutos en realizar su labor. Por tanto, se realizaron diferentes formas de optimizar la labor del servidor de dominio, donde la primera de éstas fue ajustar el horario y DNS (Sistema Dominio de Nombres) para que la búsqueda de paquetes y la transmisión de éstos sean más fluidos, generando los tiempos que se aprecian en la columna de la segunda prueba. Para disminuir aún más el tiempo de acceso al dominio, la granularidad de la implementación de las políticas fue primordial, puesto que aquellas políticas que sólo afectan al equipo están aplicadas desde el arranque del mismo, mientras que aquellas relacionadas al usuario, serán aplicadas únicamente al iniciar sesión. Luego fue necesario implementar las políticas a través de diferentes medios, de modo que cada parte del sistema contribuya al control de acceso, evitando sobrecargar la regulación. En otras palabras, si una política era cubierta de modo local en el equipo, entonces el servidor de dominio, encargado de controlar el acceso a través de la red, no aplicará dicha política, para evitar tráfico innecesario y optimizar el tráfico de paquetes en la red. La última prueba hizo diferencia puesto que se almacenó un perfil por defecto, similar al que usarán los alumnos y profesores, de modo que la mayoría de las políticas estén almacenadas en el equipo, por lo que sólo acudirá al servidor de dominio cuando se generen nuevas políticas, y el tiempo que tarda en iniciar sesión en el dominio disminuyó a 10 segundos.

Tabla 1: Promedios de tiempo que tarda el equipo en procesar el evento, las filas correspondientes al acceso local, a la red y aplicaciones no poseen diferencias dado que son eventos procesados a nivel del equipo, teniendo variaciones menos significativas en relación al acceso a la red.

Acceso	Local	Redes	Dominio	Software
1º	5	3	920	5
2º	5	3	350	5
3º	4	3	94	6
4º	4	4	43	6
5º	4	4	21	4
6º	4	4	10	4
Pruebas	**Promedio de tiempos en segundos**			

Por otro lado, se probaron las políticas, vale decir, que el usuario no pueda realizar cambios sin autorización, y de realizarlos, estos no serán almacenados permanentemente en el equipo. A su vez, se realizaron acciones que si puede realizar el usuario, como por ejemplo compartir carpetas a través de la red o descargar archivos desde Internet, los cuales eran borrados en base la configuración del control de acceso. También se contempló un ambiente similar al de una clase práctica, donde se hicieron conexiones a bases de datos, generando consultas e ingresando datos, se realizaron conexión a través de servicios Web, demostrando que el resto de los equipos puede acceder al sitio a través de la red.

Finalmente para corroborar la efectividad de la mejora propuesta, se realizó una prueba de concepto orientada a demostrar a las entidades que toman decisiones o influyen en la implantación del proyecto. La prueba realizada fue efectuada en 4 laboratorios, con un total de 40 equipos agregados al dominio, conectados a un servidor controlador, con perfiles equivalentes al de una cuenta de usuario de algún alumno o profesor. Cada equipo fue configurado, controlado localmente y remotamente mediante los diferentes recursos disponibles.

6 Conclusiones

El levantamiento y análisis de la situación actual fue realizada mediante diferentes métodos, tales como reuniones y encuestas, recogiendo datos de diferentes puntos de vista, vale decir, de los alumnos, profesores, directores y jefaturas vinculadas a la gestión y regularización de los recursos disponibles en los laboratorios, documentando los recursos existentes y describiendo sus características. Gracias a esto, es posible concluir que la información recogida durante el levantamiento y análisis de la situación actual, permitió enfocar las propuestas realizadas, formalizando, estandarizando e incluso modificando aquellos aspectos encontrados como una oportunidad de mejora.

La etapa de levantamiento y análisis de requerimientos fue realizado en base a la metodología DoRCU, con el propósito que las necesidades de los usuario puedan ser catalogados y priorizados sin mayores inconvenientes. Por lo tanto se constata que el levantamiento de requerimientos apoyado bajo la metodología DoRCU fue de gran utilidad, puesto que los diferentes pasos a seguir facilitaron la labor, haciendo que dicha etapa, siendo tan crucial para todo el proyecto, fuera validada sin mayores inconvenientes por el usuario.

En cuanto a los procesos y procedimientos que se realizaban en la Jefatura de Laboratorios, en su mayoría se ha regularizando el traspaso adecuado de información, así como también las responsabilidades de cada rol desempeñado al interior de los laboratorios y el correcto modo de realizar las diferentes labores. Por lo que es posible concluir que la documentación de los procesos y procedimientos es una mejora frente a la situación que se encontraban los laboratorios antes de este proyecto y facilita el continuo mejoramiento de éstos.

Las políticas propuestas han sido elaboradas con la base de ser complemento de aquellas establecidas por la Dirección de Informática, de modo que entre ambas se pueda otorgar mayor seguridad y control, mientras que al mismo tiempo el usuario tiene la libertad necesaria para desempeñarse normalmente al interior de los laboratorios. Por lo que se concluye que la documentación de políticas y la divulgación de éstas han generado en el usuario y el personal de laboratorios un ambiente de seguridad, dónde algunas cosas están permitidas y otras reguladas, pudiendo acceder sólo con la autorización correspondiente.

La prueba de concepto fue realizada con los recursos que se disponen en los laboratorios, haciendo uso de diferentes equipos y laboratorios, de modo que dicha prueba se acerque lo más posible a la realidad. Por lo tanto, es posible constatar que, dado los resultados de la prueba de concepto, aquellas políticas y procedimientos propuestos otorgan mayor seguridad, pudiendo controlar el acceso a la información y uso de los equipos, entregando al usuario un marco donde puede desenvolverse sin problemas, para realizar una clase práctica y al mismo tiempo respetando las políticas institucionales

Cabe mencionar que dicho proyecto cuenta con el apoyo de las entidades académicas y administrativas, vale decir, se solicitó apoyo y autorización a las entidades que de alguna forma involucraban dicho proceso, de modo que la proyección sea considerada como una realidad muy probable. Por lo que se constata que la metodología IDEAL permitió que se gestionara el apoyo de los patrocinadores, vale decir, las entidades académicas y administrativas encargadas de autorizar la implantación del sistema para el año 2010.

Para disminuir la resistencia al cambio, este proyecto contempló la participación activa del personal de laboratorios, de modo que éstos tengan la posibilidad de involucrar e integrar ideas, mejorando el resultado final obtenido. Sin embargo, esta situación tenía un alto riesgo, debido principalmente a la falta de compromiso del personal. Por lo tanto, se concluye que, dado que el riesgo asociado a la participación del personal en el proyecto fue considerado desde el comienzo, se pudo gestionar eficientemente dicha situación, evitando que este riesgo pudiese provocar un retraso en la planificación del proyecto.

6.1 Trabajos futuros

El trabajo futuro consiste en la implantación del sistema de control de acceso en los laboratorios, contemplando la integración de las partes involucradas con el sistema implementado. Así mismo, gracias a que la metodología base del proyecto contempla el continuo mejoramiento de procesos, es posible decir que otro trabajo a realizar es mejorar y perfeccionar el proceso de control de acceso, a medida que las entidades involucradas van aprendiendo en cada iteración.

Referencias

1. He, Q., y Anton, A. Requirements-based Access Control Analysis and Policy Specification (ReCAPS). En: Information and Software Technology (Vol. 51). Newton. Butterworth-Heinemann. 2009. pp 993-1009

2. Essmayr, W., Weippl, E., y Probst, S.. Role-Based Access Controls: Status, Dissemination and Prospects for Generic Security Mechanisms. En: International Journal of Electronic Commerce Research. Springer. 2004. pp.127-156.
3. Benantar, M. Access Control System, Security, Identity Management and Trust Models. New York. Springer. 2006.
4. Bidgoli, H. Handbook of Information Security, Key concepts, infrastructure, standards and protocols (Vol. I). New Jersey. John Wiley & Sons Inc. 2006
5. Ferraiolo, D. F., y Kuhn, R. Roled-Based Access Control. 2° ed. Londres, Inglaterra. Artech House. 2007
6. Layton, T. Information Security: Design, Implementation, Measurement, and Compliance. New York: Auerbach Publications. 2007
7. Escuela de Informática. Lineamientos Estratégicos. Universidad Andrés Bello, Facultad de Ingeniería. Santiago. Autor. 2008
8. Dirección de Docencia. Programación de Asignaturas. Universidad Andrés Bello, Vicerrectoría Académica. Santiago. nn. 2009
9. Jefatura De Laboratorios. Programa de Asignaturas. Universidad Andrés Bello, Escuela de Informática. Santiago. Autor. 2009
10. McFeeley, B. IDEAL: A User's Guide for Software Process Improvement. Pennsylvania. Software Engineering Institute. 1996
11. Baez, M. G. y Brunner, S. I.. Metodología DoRCU para la Ingeniería de Requerimientos. En: IV Workshop en Ingeniería de Requerimientos (WER 2001). Buenos Aires, Argentina. Universidad Nacional del Centro de la Provincia de Buenos Aires, Facultad de Ciencias Exactas, Universidad Tecnológica Nacional, Facultad Regional Buenos Aires. 2001. pp. 210-220.
12. Dirección de Informática. Políticas y Normas. Universidad Andrés Bello. Vicerrectoría de Tecnología de la Información. Santiago. Autor. 2006