UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA TÉCNICA EN INFORMÁTICA

DE GESTIÓN

PROYECTO FIN DE CARRERA:

CONTROL Y AUDITORÍA DE CORREOS ELECTRÓNICOS EN LOTUS NOTES

Autor: David Rodríguez Sánchez

Tutor: Miguel Ángel Ramos González

DEPARTAMENTO DE INFORMÁTICA

Leganés, Diciembre 2.009.

AGRADECIMIENTOS.

En primer lugar me gustaría hacer presente mi agradecimiento a Miguel Ángel, mi tutor, que siempre ha demostrado estar dispuesto a ayudarme y a dedicar a este proyecto final de carrera su tiempo, por muy ocupado que estuviese. Y porque sin su orientación y sus consejos este proyecto final de carrera nunca se hubiese concluido.

También querría agradecer a mi familia su apoyo incondicional, su comprensión a lo largo de todos estos años de carrera y porque en los momentos más difíciles siempre han tenido palabras de aliento, que conseguían que continuase hacia adelante y nunca me diese por vencido por muy mal que fuesen las cosas.

Por último me gustaría agradecer a mis compañeros de carrera y del servicio de informática, que durante el paso de los años se han convertido en grandes amigos, sus explicaciones sin las cuales no habría podido comprender algunas asignaturas, y por lo tanto, no podría haber realizado este proyecto final de carrera.

Gracias a todos.

ÍNDICE:

ÍNDICE DE IMÁGENES:

1. MOTIVACIÓN, OBJETIVOS, APORTACIONES Y CONCLUSIONES GENERALES.

1.1 INTRODUCCIÓN.

A lo largo de este punto indicaremos los motivos que nos han llevado a elegir el tema del presente proyecto final de carrera y por qué razón han sido estos los motivos y no otros los que nos han movido a la realización del presente proyecto, también indicaremos cuál ha sido el enfoque que hemos decidido dar a nuestro proyecto fin de carrera y por qué motivo hemos elegido este enfoque y no otro.

Indicaremos el ámbito de actuación y las limitaciones que dicho ámbito ha marcado en la elaboración del presente proyecto final de carrera.

Trataremos de definir los objetivos marcados al inicio del presente proyecto final de carrera, los objetivos que surgieron o que se modificaron durante la realización del presente proyecto, indicaremos la estructura del mismo e indicaremos las diferentes conclusiones a las que hemos llegado, tras la realización del proyecto final de carrera.

La finalidad de la inclusión de este punto dentro del presente proyecto final de carrera, es fijar de forma clara y que por lo tanto no deje lugar a especulaciones o dudas, sobre cuál es el objetivo que se persigue durante el presente proyecto final de carrera. También buscamos dejar claro cuáles han sido nuestras aportaciones a lo largo del presente proyecto final de carrera. Y

qué conclusiones hemos obtenido durante la realización y terminación del

presente proyecto final de carrera.

1.2 MOTIVACIÓN DEL PROYECTO.

Hemos decidido que nuestro proyecto final de carrera fuera referente a auditoría en Lotus Notes como aplicación de correo electrónico desde el punto de vista de la seguridad informática, debido a que actualmente las organizaciones tienen la necesidad de tener la certeza que sus sistemas informáticos estén debidamente protegidos de posibles ataques externos y entre sus sistemas informáticos el sistema de correo electrónico es especialmente prioritario para un gran número de organizaciones.

Muchas organizaciones, indistintamente de cuál sea su área de negocio, basan gran parte de su actividad en la recepción y envío de correos electrónicos, ya sea para recibir pedidos, para realizar encargos, notificaciones, etcétera.

Dentro de las aplicaciones de correo electrónico comerciales una de las más extendidas es la aplicación Lotus Notes junto con las herramientas de correo electrónico de Microsoft, en nuestro caso hemos decidido decantarnos por la aplicación Lotus Notes, porque existe menos documentación respectiva a la configuración y posibles medidas de seguridad que de las herramientas comerciales de Microsoft de correo electrónico y por lo tanto hemos considerado que sería más interesante y útil para los posibles lectores del proyecto final de carrera, que la aplicación evaluada y auditada en el actual proyecto final de carrera fuera la aplicación Lotus Notes.

Por lo tanto, nuestro proyecto final de carrera tiene como finalidad conseguir que los lectores del mismo puedan comprobar que la instalación y configuración de la aplicación Lotus Notes, dentro de cualquier organización,

garanticen unos mínimos de seguridad tanto en la recepción y envío de correos electrónicos, como en el acceso a la aplicación Lotus Notes.

Hemos decidido darle al presente proyecto final de carrera un enfoque más didáctico, en lugar de darle un enfoque más técnico, ya que de esta forma pensamos que el presente proyecto final de carrera será entendible por cualquier posible lector del mismo e igualmente de esta forma, dicho lector, podrá a través de unas comprobaciones básicas, y desde nuestro punto de vista, bastante simples evaluar de forma clara y concreta la instalación y configuración de la aplicación Lotus Notes dentro de cualquier organización, sea cual sea su tipo de negocio y su estructura organizativa.

El espíritu del presente proyecto fin de carrera es más bien formativo, es decir, que la idea principal del mismo es que cualquier posible lector pueda comprender todo lo que en el presente proyecto se dice, aunque el lector no tenga ningún tipo de formación en auditoría o en informática.

Debido a que no podremos disponer de ninguna organización en la que se encuentre instalada la aplicación Lotus Notes, trabajaremos con la aplicación instalada en un único equipo personal, además la versión que utilizaremos durante todo el desarrollo del proyecto final de carrera será una versión de evaluación de la aplicación Lotus Notes 8.5.

Teniendo en cuenta el ámbito de actuación para el presente proyecto final de carrera descrito con anterioridad, tendremos limitaciones en cuanto al número de equipos que probar, diferentes versiones de sistema operativo, diferentes tipos de usuario, imposibilidad de comprobar la aplicación de las políticas internas, etcétera.

1.3 OBJETIVOS.

A lo largo de este punto definiremos los objetivos que nos marcamos al comienzo del presente proyecto final de carrera, teniendo en cuenta, en todo momento, cuál era la finalidad del proyecto.

Uno de los objetivos de este proyecto era que toda persona que lo abordase pudiera comprenderlo, si no totalmente al menos en su mayoría, independientemente de cuáles sean sus conocimientos en informática o en auditoría. Consideramos muy importante que el proyecto final de carrera sea comprensible para todos los lectores del mismo, puesto que de esta forma conseguiremos que un mayor número de personas se familiaricen con los conceptos y términos de seguridad informática y de auditoría informática, y con la aplicación de dichos conceptos al correo electrónico, y en especial a la aplicación Lotus Notes como cliente de correo electrónico.

Otro de los objetivos de este proyecto final de carrera era conseguir que los lectores del mismo, consiguiesen familiarizarse con la seguridad informática y comprendiesen que es de vital importancia aplicar todos sus conceptos, sea cuál sea el ámbito laboral o personal, en que los lectores interactúan con sistemas informáticos. Lo que pretendemos conseguir es que el lector adquiera una base sólida en seguridad informática, que le permita comprobar la seguridad de forma genérica tanto de su equipo personal como de su equipo de trabajo, también lo que pretendemos es crear en el lector la suficiente inquietud intelectual que le conlleve intentar completar sus conocimientos en seguridad informática.

Otro de los objetivos que se perseguían durante la elaboración del presente proyecto final de carrera era conseguir que los lectores del mismo entendiesen el significado y la utilidad de la auditoría, y en particular de la auditoría informática. De esta forma se intenta que el lector adquiera los suficientes conocimientos sobre auditoría informática, que le permitan saber qué puntos son los más débiles de los equipos informáticos con los que trabaja y actuar en consecuencia.

Otro objetivo que se perseguía durante la elaboración de este proyecto es que el lector se familiarice con la normativa vigente aplicable a seguridad informática, auditoría informática y al correo electrónico. De esta forma pretendemos que los lectores no infrinjan por desconocimiento, normativas, estándares ni leyes durante cualquier tipo de actividad que realice con equipos informáticos, ya sea para uso personal, laboral o lúdico, y si se da el caso que alguno de ellos infringen la normativa legal sepan cuáles pueden ser las consecuencias de sus actos.

Otro de los objetivos que se perseguían durante la elaboración del presente proyecto final de carrera era que los lectores se familiarizasen con los componentes del correo electrónico y de los gestores de correo electrónico, y entendiesen de forma general su funcionamiento y cuál es su estructura general. De esta forma pretendemos que los lectores sepan cuál es el funcionamiento de un sistema de correo electrónico, cuáles son sus características principales y cuáles son sus principales debilidades o inconvenientes.

El principal objetivo del presente proyecto final de carrera era realizar una auditoría informática, desde el punto de vista de la seguridad, de la aplicación Lotus Notes como gestor de correo electrónico, y que cualquier lector que abordase el proyecto fuese capaz de entender el significado general del mismo y pueda extraer sus propias conclusiones en relación a cómo debería estar instalado y configurado un sistema de correo electrónico, al que se accediese con el cliente de correo electrónico de la aplicación Lotus Notes. De esta forma pretendemos que si alguno de los lectores envía o recibe correos con la aplicación Lotus Notes o debe comprobar su correcta instalación o configuración, pueda basarse en el presente proyecto final de carrera para comprobar que los parámetros de la configuración, del cliente de correo electrónico de la aplicación Lotus Notes, son correctos y en el caso que existiese algún tipo de normativa (interna o legal) o estándar aplicable comprobar que la configuración del cliente de correo electrónico de la aplicación Lotus Notes también los cumple.

1.4 ESTRUCTURA DEL PROYECTO.

El presente proyecto final de carrera consta de siete puntos o capítulos, dos anexos, un glosario de términos y las referencias bibliográficas.

En el punto 1 del presente proyecto final de carrera tratamos de hacer comprender al lector cuáles han sido los motivos que nos han llevado a escoger el tema del presente proyecto final de carrera, indicamos cuales han sido los principales objetivos del presente proyecto, cuál es la estructura del proyecto y cuáles han sido las conclusiones que se han obtenido tras su realización y nuestras aportaciones.

En el punto 2 del presente proyecto final de carrera realizamos una breve introducción a los sistemas de correo electrónico, a los clientes de correo electrónico y los protocolos que se utilizan para el envío y recepción de correo electrónico.

En el punto 3 del presente proyecto final de carrera explicamos qué es la seguridad informática, qué puntos se pueden considerar básicos para la seguridad informática, cuáles son las principales amenazas, vulnerabilidades y las medidas de protección frente a las mismas, explicamos los conceptos de criptografía, firma digital y de políticas de seguridad.

En el punto 4 del presente proyecto final de carrera hacemos un breve resumen, haciendo especial hincapié en los puntos más relacionados con el correo electrónico, de la ley orgánica de protección de datos, de la ley de servicios de la sociedad de la información, del estándar ISO 27002, de qué es y en qué consiste ISACA y por último enumeramos las principales conclusiones extraídas durante la realización del punto o capítulo 4.

En el punto 5 del presente proyecto final de carrera definimos qué es la auditoría informática, qué son los controles internos, la figura del auditor informático, los métodos, técnicas y herramientas más utilizadas durante la realización de una auditoría informática, qué es el programa de trabajo, qué es el informe de auditoría, en qué consiste una auditoría de seguridad, de aplicaciones, de seguridad en las comunicaciones y en el correo electrónico.

En el punto 6 del presente proyecto final de carrera realizamos una evaluación de los posibles riesgos a los que puede estar sometido la aplicación Lotus Notes como cliente de correo electrónico, indicamos cómo se puede comprobar que la configuración del cliente de correo electrónico de Lotus Notes evita los posibles riesgos, indicamos cuáles podrían ser las preguntas a realizar al personal de la organización en la que se encontrase instalada la aplicación Lotus Notes para comprobar hasta qué punto se han tenido en cuenta los posibles riesgos.

En el punto 7 del presente proyecto final de carrera realizamos un prototipo de aplicación informática de cuestionarios, el cual permitiría realizar los cuestionarios directamente sobre un equipo informático e indicamos un posible ejemplo de realización de un cuestionario a través del prototipo de la aplicación.

En el anexo a del presente proyecto final de carrera hacemos un amplio resumen del estándar ISO 27002.

En el anexo b del presente proyecto final de carrera hemos realizado una pequeña guía de instalación de la aplicación Lotus Notes como cliente de correo electrónico.

Podemos decir que el presente proyecto final de carrera está compuesto por dos bloques claramente diferenciados, un primer bloque de corte muy didáctico, en el que se explican los principales conceptos del correo electrónico, la seguridad informática, la legislación vigente aplicable al presente proyecto y de la auditoría informática. Y un segundo bloque más práctico en que se muestran los posibles puntos débiles de la aplicación Lotus Notes y se indican las medidas oportunas para solventar dichas debilidades y se indica la forma correcta de realizar la instalación de la aplicación Lotus Notes como cliente de correo electrónico.

1.5 APORTACIONES.

A lo largo de este punto indicaremos cuáles son las aportaciones que se realizan a lo largo del presente proyecto final de carrera en relación con el tema del mismo, es decir, en relación con el correo electrónico, Lotus Notes, auditoría, seguridad, etcétera.

La principal aportación sobre el correo electrónico de este proyecto final de carrera, es conseguir que el lector aunque no esté familiarizado con las nuevas tecnologías ni con internet, entienda el concepto de correo electrónico la estructura del mismo y cuál es su funcionamiento. Aunque existe mucha documentación sobre el correo electrónico, tanto para expertos como para principiantes, existen muy poco manuales o libros que de forma clara y concisa definan la estructura del correo electrónico y su funcionamiento, lo que desde nuestro punto de vista sí somos capaces de realizar durante el presente proyecto final de carrera. La otra gran aportación en relación con el correo electrónico es que a lo largo del presente proyecto final de carrera se indica que aspectos de los clientes de correo hay que tener en cuenta, para que el envío y recepción de correos electrónicos se haga de forma segura, se pueda autentificar el remitente del correo y se pueda asegurar que el contenido del mismo no ha sido modificado desde que su emisor lo elaboró y el receptor o receptores lo recibieron.

La aportación más importante sobre la seguridad informática de este proyecto final de carrera, es que se consigue hacer un buen resumen y bastante completo, de qué es la seguridad informática, para qué se utiliza y qué puede prevenir. Aunque existe mucha literatura, normativa y estándares sobre la

seguridad informática es difícil encontrar un único documento en el que se resuman el concepto, las principales características, técnicas y métodos de la seguridad informática utilizando un lenguaje lo suficientemente llano y asequible como para que cualquier lector pueda comprender el significado del mismo, sin que se requiera que el lector posea unos conocimientos técnicos muy elevados. Desde nuestro punto de vista todas estas afirmaciones se cumplen a lo largo del presente proyecto final de carrera.

La aportación más importante del presente proyecto final de carrera sobre el tema de la normativa y de los estándares es que se consigue hacer un resumen bastante completo de la normativa y estándares aplicables al correo electrónico dentro del marco legal español y europeo, mediante la utilización de un lenguaje asequible para cualquier persona y evitando en la medida de lo posible la jerga legal. Aunque existen un gran número de publicaciones respecto a este tema, suelen ser más extensas y utilizar un lenguaje más legislativo y por lo tanto su lectura es más pesada y complicada para lectores no acostumbrados a leer ese tipo de documentación, además muchos de los estándares y/o normas y RFCs que se pueden aplicar al correo electrónico y a las nuevas tecnologías se encuentran en inglés o su traducción al castellano es muy pésima, por lo que la lectura de los mismos se hace todavía más complicada y liosa para los lectores que no posean altos conocimientos técnicos en la materia o sean expertos traductores del inglés al castellano.

La principal aportación del presente proyecto final de carrera sobre el tema de auditoría es que se consigue hacer un resumen bastante claro y conciso de qué es una auditoría, en qué consiste, qué técnicas y herramientas utiliza, y qué personas intervienen en ella. Aunque sobre este tema existe mucha

información, creemos que nuestro resumen consigue algo que el resto de publicaciones no consiguen, y es que todo lo referido anteriormente se hace utilizando un lenguaje simple y con el suficiente nivel de explicación, para que cualquier personal que lea el proyecto pueda entender en qué consiste una auditoría y cuál es su utilidad, sin necesidad de que posea conocimientos en la materia. Otra de las aportaciones que se realizan sobre el tema de la auditoría es que se hacen un pequeño resumen sobre la auditoría de la seguridad y su importancia para cualquier organización, también se realizan resúmenes sobre la auditoría de la seguridad en las aplicaciones, en las comunicaciones y en el correo electrónico, al igual que en el caso anterior estos resúmenes se hacen utilizando un lenguaje simple para conseguir el mismo objetivo que en el caso anterior, es decir, que cualquier persona que tenga acceso al presente proyecto final de carrera y lo lea pueda entender en qué consiste una auditoría de seguridad, ya sea sobre una aplicación, sobre comunicaciones, sobre accesos, etcétera y entienda su importancia para cualquier organización, esto no queda siempre claro en toda la documentación existente sobre este tema, ya que aunque en la mayoría de los casos el objetivo de la documentación es que los lectores entiendan qué es una auditoría y cuál es su importancia, debido al lenguaje técnico utilizado únicamente las personas con una amplia base de conocimientos en informática, en seguridad o en auditoría son capaces de entender por entero dicha documentación, y creemos que en nuestro caso si conseguimos que cualquier lector entienda la importancia de la auditoría y en qué consiste.

El resto de aportaciones del presente proyecto final de carrera están estrechamente relacionadas con la aplicación Lotus Notes. Una de las

principales aportaciones en relación con Lotus Notes, es que a lo largo del presente proyecto se explica cómo debe estar configurada la aplicación Lotus Notes para que sea un gestor de correo electrónico seguro, tanto para el envío y recepción de correos, cómo para el acceso a la propia aplicación. En relación a cómo debe de estar configurada la aplicación Lotus Notes para que sea un gestor de correo electrónico seguro, no existe demasiada documentación y la existente se encuentra en su mayoría en inglés, pues casi toda la documentación forma parte o de los redbooks de IBM sobre la aplicación Lotus Notes o de la ayuda de la propia aplicación (en el caso que la aplicación se encuentre en castellano la ayuda también se encontrará en castellano), pero en ambos casos la documentación no indica que parámetros de la aplicación hay que modificar o que valor han de tener dichos parámetros para que la aplicación Lotus Notes sea considerada como un gestor de correo electrónico seguro, sino que únicamente indica dónde se pueden modificar los parámetros, que posibles valores pueden tomar dichos parámetros y qué función o utilidad poseen esos parámetros dentro de la aplicación Lotus Notes, por lo tanto hemos pensado que sería muy interesante incluirlo en el presente proyecto final de carrera, para que todo lector del mismo sepa que aspectos de la aplicación Lotus Notes se deben tener en cuenta para que esta sea considerada segura.

Otra aportación del presente proyecto final de carrera en relación con la aplicación Lotus Notes es que a lo largo del mismo se indica cómo se puede comprobar que la configuración existente de la aplicación Lotus Notes es segura como gestor de correo electrónico. Obviamente en este caso tampoco existe demasiada documentación respecto a cómo comprobar que una instalación de la aplicación Lotus Notes es segura como gestor de correo

electrónico, y por lo tanto hemos decidido incluirlo en el presente proyecto final de carrera para que todo lector del mismo que se encuentre con la aplicación Lotus Notes instalada pueda comprobar de forma rápida y sencilla que la configuración de la aplicación se puede considerar correcta desde el punto de vista de la seguridad en la aplicación Lotus Notes como gestor de correo electrónico. La otra gran aportación del presente proyecto final de carrera respecto a la aplicación Lotus Notes es que a lo largo del mismo se indica cómo se puede realizar una instalación desde cero de la aplicación Lotus Notes para que dicha instalación se pueda considerar segura como gestor de correo electrónico. Respecto a este tema tampoco existe apenas documentación, y por lo tanto hemos creído muy interesante incluirlo en el presente proyecto final de carrera, para que todo lector del mismo y que quiera instalar la aplicación Lotus Notes pueda hacerlo de una forma sencilla y teniendo presente qué parámetros debe configurar y de qué forma para que la instalación de la aplicación Lotus Notes, como gestor de correo electrónico, sea considerada como segura.

Otra de las aportaciones del presente proyecto final de carrera es en relación a las posibles preguntas que se podrían realizar en una auditoría para averiguar si la configuración de la aplicación Lotus Notes como gestor de correo electrónico se puede considerar segura. Al igual que en los casos anteriores no existe demasiada documentación al respecto por no decir que en este caso es prácticamente inexistente, por lo que hemos creído interesante introducirla en el presente proyecto final de carrera, para que cualquiera de los lectores del presente proyecto que tuviese que realizar una auditoría sobre la seguridad de

la aplicación Lotus Notes como gestor de correo electrónico, pueda basarse en dichas preguntas para realizar sus entrevistas y cuestionarios.

Podemos decir que la última aportación del presente proyecto es la elaboración de un prototipo de aplicación de cuestionarios que facilite la labor a todo encuestador o auditor. Es un prototipo bastante abierto y que permite gran versatilidad a la hora de crear preguntas pues admite bastantes tipos de preguntas. Aunque en la actualidad existen muchas aplicaciones de este tipo y que también permiten múltiples tipos de preguntas, hemos creído interesante introducir un prototipo propio de aplicación de cuestionarios para añadir un cuestionario de ejemplo sobre esta aplicación y que el lector pueda comprobar la importancia de utilizar aplicaciones a la hora de realizar cuestionarios, ya que de esta forma toda la información de los mismos queda inmediatamente informatizada y no es necesario pasar posteriormente los resultados de las encuestas a los equipos informáticos, para su procesamiento.

1.6 CONCLUSIONES GENERALES.

Tras la realización del presente proyecto final de carrera hemos obtenido varias conclusiones que hemos creído oportuno compartir con todos los lectores del proyecto, para que puedan comparar sus conclusiones obtenidas con las que mostramos a continuación.

Podemos considerar que la aplicación Lotus Notes como cliente de correo cumple con lo estipulado a lo largo del título VIII del reglamento de la ley de protección de datos en materia de niveles de seguridad, ya que permite el cifrado a tres niveles diferentes. Por lo que los niveles de cifrado de la aplicación Lotus Notes se corresponden, perfectamente, con los tres niveles de seguridad estipulados en el título VIII del reglamento que desarrolla la ley de protección de datos. Es importante que destaquemos que el cifrado de los datos en la aplicación Lotus Notes se hace de forma manual, por lo que deberá ser el propio responsable de los datos quien decida qué nivel de cifrado se le debe asignar a la información, teniendo en cuenta sus propias necesidades y lo estipulado en el reglamento de la ley orgánica de protección de datos. Dentro de la información que debería tener el mayor grado de cifrado podemos destacar datos personales, cualquier tipo de referencia a contraseñas o usuarios de conexión a otros equipos o aplicaciones, listas con información importante para la organización,…

Podemos considerar que cualquier organización que facilite a sus empleados cuentas de correo electrónico corporativas es una organización suministradora de servicios, y por lo tanto ha de estar sujeta a la ley de servicios de sociedad de la información, y no puede ignorar lo que en dicha ley se estipula. Siguiendo

este mismo razonamiento, si la organización obligase a sus empleados a acceder a su correo corporativo a través del cliente de correo de la aplicación Lotus Notes, la organización debería poder asegurar la privacidad y veracidad de los correos electrónicos, igual que cualquier otra organización suministradora de servicios. Por lo tanto, la propia organización deberá encargarse de verificar que la configuración del cliente de correo de la aplicación Lotus Notes cumple con lo estipulado en la ley de servicios de la sociedad de la información, al igual que todos los servidores y aplicaciones que intervengan en el servicio de correo electrónico.

Teniendo en cuenta las premisas de ISACA y del estándar ISO 27002 podemos considerar que son igual de importantes los medios humanos que los medios técnicos a la hora de asegurar el correcto funcionamiento de cualquier sistema, ya que por muy bueno que sea un sistema, si la persona encargada de administrarlo o gestionarlo no tiene los suficientes conocimientos técnicos o simplemente es una persona deshonesta que pretende obtener algún tipo de beneficio gracias a su posición. También para el personal de auditoría se cumple este axioma, ya que por muy buenas herramientas de auditoría que se posean y muy buenos manuales, si el auditor es una persona poco habilidosa, con poca experiencia o especialmente deshonesta, no servirán de nada las herramientas y los manuales.

Teniendo en cuenta lo expuesto a lo largo del presente proyecto final de carrera podemos considerar que el cliente de correo electrónico de la aplicación Lotus Notes, con una configuración correcta, cumple con todas las disposiciones aplicables, tanto legales como a nivel de estándares, a un cliente de correo electrónico desde el punto de vista de la seguridad. Ya que se puede

asegurar el correcto cifrado de la información almacenada en el cliente de correo, permite el envío y recepción de correos autentificados, permite firmar los correos enviados, no permite el acceso al cliente sin introducir un usuario y una contraseña válidos, tampoco permite el acceso a ninguna información sin introducir usuario y contraseña válidos. También podemos decir del cliente de correo electrónico de la aplicación Lotus Notes que gracias a sus múltiples opciones permite una gran variedad de configuraciones a nivel de seguridad, que pueden ser muy útiles para la creación de diferentes perfiles de usuarios, en relación a la relevancia de la información que manipulen los distintos usuarios para la organización, aunque es conveniente destacar que los perfiles de usuario podrían ser modificados por los propios usuarios, ya que el cliente de correo electrónico de la aplicación Lotus Notes permite que los propios usuarios modifiquen muchas de las opciones de seguridad.

2. CORREO ELECTRÓNICO.

2.1 INTRODUCCIÓN.

Hemos creído conveniente añadir este punto en la memoria del proyecto final de carrera, porque al tratarse de una auditoría sobre un gestor de correo electrónico, en el caso que nos ocupa el gestor de correo es Lotus Notes, hemos pensado que en primer lugar deberíamos dar unas nociones básicas sobre el funcionamiento del correo electrónico, su historia, los protocolos que intervienen en su funcionamiento y de los clientes de correo electrónico que son los que nos permiten visualizar los correos electrónicos recibidos y realizar el envío de los mismos. De esta forma lo que pretendemos es que nuestro proyecto final de carrera sea fácilmente comprensible, incluso por personas que no tengan una gran base en la materia que nos ocupa.

A continuación procedemos a hacer un pequeño resumen sobre la aparición y evolución del correo electrónico hasta nuestros días.

Aunque pueda parecer contradictorio el origen del correo electrónico es anterior al propio origen de internet, y sin su aparición probablemente internet no existiría, o al menos no sería igual a la que conocemos.

En 1.961 en una demostración en el MIT de Massachusetts se utilizó un sistema que permitía a usuarios remotos conectarse a un terminal y almacenar ficheros en el disco de forma remota, esto dio paso a una nueva forma de intercambio de información. A partir de 1.965 comenzó a usarse el correo electrónico en una supercomputadora de tiempo compartido; pero no fue hasta el año siguiente cuando comenzó a extenderse en las redes de computadores.

Hasta 1.971 no se realizó el primer envío de correo electrónico o e-mail, tal y como lo conocemos en la actualidad. Cuando Ray Tomlinson, que trabajaba en el proyecto ARPANET del gobierno norteamericano, desarrollo un programa que permitía dejar mensajes en las distintas computadores pertenecientes a dicho proyecto, para que los desarrolladores del mismo pudieran comunicarse de forma directa sin necesidad de usar el teléfono, el correo postal o verse obligados a reunirse.

Tomlinson llegó a la conclusión de que necesitaba algún carácter para separar el nombre de usuario y el nombre de la computadora en la que se encontraba alojado el buzón de correo, decidió que la @ sería el mejor carácter para utilizar como divisor, ya que ningún nombre ni apellido la contiene y además es un carácter internacional.

Pero no fue hasta el año 1.977 cuando se sentaron las bases definitivas del correo electrónico, ya que fue en este año cuando apareció la RFC 733, en la que se detallan todas las especificaciones para el envío y recepción de correo electrónico. Esta RFC sufrió una revisión en 1.982 y fue sustituida por la actual RFC 822.

Pero hasta el año 1.994 no apareció la RFC 1725, en la que se especifican los parámetros del protocolo POP3, tan utilizado en nuestros días en los gestores de correo electrónico y en los web mails, tan extendidos actualmente.

2.2 ¿QUÉ ES EL CORREO ELECTRÓNICO?

En primer lugar trataremos de dar una definición genérica y fácilmente comprensible del significado de correo electrónico, para proseguir a continuación con una definición más técnica.

El correo electrónico no es más que una carta enviada en formato electrónico a través de un ordenador y prescindiendo del soporte habitual de las cartas, el papel y la tinta. Por lo tanto, han de tener muchas similitudes. Por ejemplo, cuando escribimos una carta, en el sobre debemos poner la dirección del destinatario y el remitente de la carta, pues con el correo electrónico pasa exactamente lo mismo, debemos poner la dirección de correo electrónico del destinatario para que el correo electrónico llegue a la persona que va dirigido, un asunto para que el destinatario tenga una idea del contenido del correo electrónico, sin que se vea obligado a leerlo. También aparece la dirección del correo del remitente aunque actualmente no es necesario que el remitente la teclee, ya que los actuales gestores de correo electrónico se encargan de añadirla automáticamente. También ofrecen la posibilidad de adjuntar archivos, que es como si realizáramos un envío de un paquete a través del correo postal.

Ahora procederemos a dar una definición más técnica y compleja de qué es el correo electrónico:

El correo electrónico no es otra cosa que una aplicación vía internet para el intercambio de mensajes entre distintas personas u ordenadores, estos mensajes pueden ser únicamente de texto o llevar adosados ficheros adjuntos. Por lo tanto, para poder hacer uso de esta aplicación es necesario que podamos tener acceso a internet, puesto que internet es el medio de transmisión de los correos electrónicos. El sistema de correo electrónico no es sólo el software que

instalamos en nuestro ordenador o la página de internet que utilizamos para enviar y consultar nuestro correo, sino que consta de múltiples servidores, cada uno con unas funciones y requerimientos específicos, las cuales procederemos a explicar a continuación.

Hay que tener en cuenta que los sistemas de correo electrónico actuales tienen una estructura cliente-servidor, es decir, hay una parte del sistema que se ejecuta en los servidores de correo, y que es ajena al usuario y su ordenador, y otra parte del sistema se debe ejecutar en el lado del cliente, es decir, se ejecuta en el propio ordenador del usuario, ya sea a través de un gestor de correo tradicional de escritorio o un gestor de correo web, de los más recientes, aunque para el usuario es totalmente transparente.

En primer lugar describiremos la parte de correo electrónico del cliente:

Es necesario un agente de usuario (User Agent) también conocido como correo del agente de usuario (Mail User Agent), que es la parte del correo electrónico que se ejecuta en el lado del usuario, esta parte es totalmente transparente para el usuario, ya que es el propio gestor de correo electrónico de escritorio o correo web quién se encarga de su gestión. Este Agente de Usuario es el encargado de gestionar la interfaz de usuario, de controlar las funcionalidades de creación, envío y recepción de mensajes, a través de ella se realiza la configuración de la conexión (tanto de puertos como de protocolos), y gestiona las bandejas de entrada y salida de correo.

A continuación vamos a describir la parte de correo electrónico del servidor:

Es necesario tener una estructura de ficheros para almacenar y gestionar los buzones de correo de todos los usuarios registrados en el servidor de correo. También es necesario un Agente de Usuario de servidor que se encarga de

interactuar con el Agente de Usuario del cliente. Es necesario un almacén de mensajes (Message Store), para tener correctamente ordenados los mensajes en los buzones de los usuarios correspondientes. Por último, es necesario un Agente de Transferencia de Mensajes (MTA), que es el encargado de realizar los envíos y recepciones de los distintos correos.

Una estructura válida de cliente-servidor para el correo electrónico podría ser la siguiente:

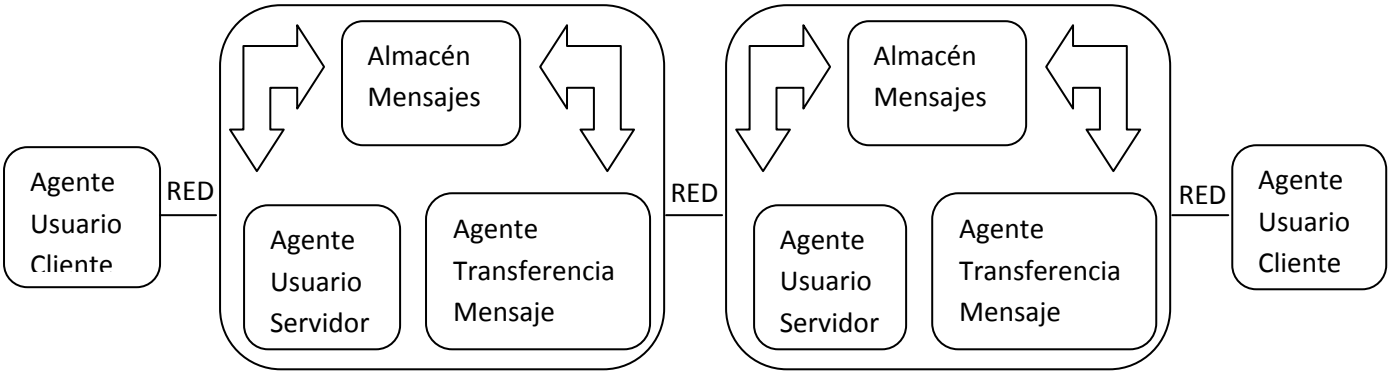

Figura 2.1: Ejemplo funcionamiento cliente servidor de correo electrónico.

Debido a qué el correo electrónico necesita como medio de difusión internet la estructura de los mismos está bien definida, básicamente constan de una serie de cabeceras, el cuerpo del propio mensaje y los ficheros adjuntos. Esta definición viene dada en la RFC 822.

Dentro de las cabeceras podemos dividir en tres partes las cabeceras, las cabeceras insertadas por el servidor en la transferencia del mensaje, las cabeceras insertadas por el Agente de Usuario del cliente y las cabeceras definidas por el propio usuario. A continuación procedemos a realizar una descripción de las mismas:

- **Cabeceras insertadas por el servidor.**

  Dentro de estas cabeceras podemos destacar: **From** (dirección de correo de la persona que envió el mensaje), **To** (dirección de correo de la persona a la que va destinado el mensaje), **CC** (lista de direcciones de correo a las que va destinado el mensaje de forma secundaria), **Received** (ruta por los distintos servidores que debe seguir el mensaje a través del sistema de transferencia) y **Return-Path** (nombre del último agente de transferencia de mensaje por el que ha pasado el mensaje).

- **Cabeceras insertadas por el Agente de usuario.**

  Dentro de estas cabeceras podemos destacar: **Sender** (dirección de correo de la persona que envía el mensaje), **Date** (Día y hora del Agente de Usuario en el momento que se envió el correo), **Message-Id** (identificador único del mensaje, asignado por el Agente de Usuario), **Reply-to** (dirección de correo a la que se debe enviar la contestación del mensaje) y **Subject** (Título representativo del mensaje, es elegido por el emisor del mensaje).

- **Cabeceras definidas por el usuario.**

  Dentro de estas cabeceras podemos encontrar todo tipo de información suelen ser del tipo **X-NumeroTelefono**, **X-DireccionPostal**,**…** y representan información adicional añadida por el emisor del mensaje.

2.3 CLIENTES DE CORREO ELECTRÓNICO

Un cliente de correo electrónico no es otra cosa que un programa de ordenador que nos permite enviar, recibir y leer los correos electrónicos que nos envían, por lo tanto para poder disfrutar de todas sus funcionalidades, el cliente de correo electrónico de escritorio que tengamos instalado en nuestro ordenador debe ser compatible con nuestro sistema operativo. Y en el caso que usemos un cliente de correo electrónico web deberemos asegurarnos que nuestro navegador web es totalmente compatible con el cliente de correo electrónico web, también llamado webmail.

Originariamente los clientes de correo electrónico fueron concebidos únicamente para poder recibir y enviar correos electrónicos de forma local, aunque en la actualidad son mucho más, ya que permiten tener bases de datos con los teléfonos, direcciones postales, nombres y apellidos, … de nuestros contactos, también permiten tener calendario, citas, notas, … Actualmente los clientes de correo también ofrecen la posibilidad de tener ficheros de firmas, para que se adjunten al correo y de esta forma darle más autenticidad. También permiten la creación de filtros de correo, para que los mensajes que cumplan una serie de condiciones sean automáticamente borrados o movidos a determinadas carpetas, algunos de los servicios antispam únicamente son una serie de filtros creados por el distribuidor que impiden que ciertos correos se entreguen en el buzón del usuario.

Los clientes de correo electrónico tradicionales suelen utilizar como formatos de buzón mbox o maildir, que no son más que dos formatos para almacenar de forma local o en el propio servidor nuestros correos electrónicos y que además permiten la exportación, importación e incluso la realización de

copias de seguridad de las carpetas locales en las que almacenamos nuestro correo electrónico. A diferencia de lo que ocurre con los protocolos de transferencia de correo que están definidos en las RFCs correspondientes, como veremos más adelante, el formato para el almacenamiento de correos no está definido en ninguna RFC, por lo que su implementación queda abierta para que cada cliente de correo electrónico lo implemente de la forma que más le convenga al desarrollador.

- **mbox:** La mayor particularidad de este formato es que todos los mensajes del buzón del usuario se encuentran en un único fichero. Cada mensaje comienza por “FROM” y acaba con una línea en blanco. Debido a estas características, este formato fue muy popular durante algún tiempo, ya que permitía parametrizar los correos con bastante facilidad, es decir, se podían utilizar múltiples programas de procesado de texto, lo que para los desarrolladores era muy cómodo. Aunque también tiene un gran inconveniente, ya que al almacenarse los correos en un único fichero podría darse el caso que el fichero se corrompiese al ser accedido por varios procesos simultáneamente, es decir, que un proceso estuviese leyendo el fichero y a la vez otro proceso distinto lo estuviese escribiendo. Debido a este problema los desarrolladores debieron crear un sistema de bloqueo que evitase que el fichero se corrompiese.
- **maildir:** La mayor particularidad de este formato en comparación con mbox, es que en el lugar de tener un único fichero para almacenar los mensajes, cada mensaje se almacena en un único fichero independiente del resto de mensajes. Usa una estructura muy

simple de carpetas. De la carpeta Maildir de cada usuario cuelgan las carpetas new, tmp y cur. El procesado del mensaje es el siguiente.
En primer lugar el mensaje se almacena en la carpeta tmp hasta que el cliente de correo electrónico enlaza el mensaje desde tmp a new.
Cuando el usuario inicia sesión con su cliente de correo, éste se encarga de mover todos los correos desde new a cur.
Debido a esta estructura de carpetas y a que cada mensaje se almacena en un fichero diferente no se deberían producir problemas de concurrencia de procesos; pero a decir verdad no es fiable en el 100% de los casos, ya que si se está modificando Maildir a la vez que se está obteniendo el listado de los mensajes, puede producirse un error de lectura y que alguno de los mensajes se pierda temporalmente.

Los clientes de correo electrónico no necesitan realizar labores de transporte para enviar correos, ya que únicamente se limitan a entregar el correo electrónico al agente de transferencia de correo del proveedor de correo electrónico que nos facilita el servicio. El agente de transferencia es el encargado de transferir el correo electrónico desde el ordenador del emisor hasta el buzón de correo del receptor en su servidor de correo.

Los clientes de correo electrónico actuales soportan los protocolos de transferencia de correo IMAP y POP3, ya que estos protocolos son los encargados de realizar la comunicación con el agente de transferencia de correo remoto localizado en el servidor del proveedor de correo electrónico que nos suministra el servicio de correo electrónico. La principal diferencia entre estos dos protocolos es que mientras IMAP está optimizado para que los correos

electrónicos se almacenen directamente en el servidor, consumiendo de esta manera la cuota de correo asignada para el usuario, POP3 está diseñado para que los correos electrónicos sean descargados a local por el usuario a través de su cliente de correo electrónico.

La mayoría de los clientes de correo electrónico utilizan el protocolo SMTP para realizar los envíos de correo electrónico, también soportan el estándar MIME, que es utilizado para enviar ficheros binarios adjuntos al correo, es decir, este estándar se encarga de adjuntar documentos al correo electrónico.

Los cuatro protocolos mencionados anteriormente los veremos con más detalle en el siguiente punto de esta memoria.

En la actualidad, y debido a la proliferación de la banda ancha, han aparecido clientes web de correo electrónico o webmail, los cuales han desplazado a los clientes de correo electrónico de escritorio tradicionales. El funcionamiento de estos webmails es básicamente igual al de los clientes de correo de escritorio a excepción de que no es necesario instalar ningún programa de ordenador, a excepción de un navegador web, para poder leer o enviar correos electrónicos.

Entre los clientes de correo electrónico web más utilizados podemos destacar gmail, hotmail o yahoo, aunque existen muchos más.

Entre los clientes de correo electrónico tradicionales podemos destacar outlook, thunderbird, Lotus Notes, aunque al igual que en el caso de los clientes web existen muchos más.

2.4 PROTOCOLOS DE CORREO ELECTRÓNICO.

Para el correcto funcionamiento de los servidores de correo electrónico y los clientes de correo electrónico se implementan una serie de protocolos que procederemos a explicar en detalle a continuación.

- **SMTP (Simple Mail Transfer Protocol)**

  Es el protocolo simple de transferencia de mensajes, es decir, es el protocolo encargado de gestionar los envíos de correo electrónico entre los distintos servidores de correo, para ello utiliza el puerto 25 de comunicación TCP/IP. Se realiza una comunicación cliente-servidor, a través de telnet, en formato de texto plano ASCII, en la que se indican las características y configuraciones necesarias para que el servidor de correo pueda realizar el envío, es decir, direcciones de correo (destinatario y emisor), el propio mensaje,…
  La RFC en la que se indicaban las características de este protocolo era la 821, aunque actualmente ha sido reemplazada por la 2821.
  Este protocolo permite tener un servidor de correo centralizado para múltiples usuarios. Los mensajes que se envían a través de este protocolo deben tener una forma específica, la cual viene determinada por la RFC 822, aunque actualmente ha sido reemplazada por la RFC 2822.

- **POP (Post Office Protocol)**

  Es el protocolo de oficina postal, es decir, desempeña las mismas funciones que una oficina postal de correos, es utilizado para conectarse al servidor de correo en el que se alojan nuestros mensajes de correo y así tener acceso a los mismos. Este protocolo

utiliza el puerto 110 de comunicación TCP/IP. Las RFCs en las que se indican las características de este protocolo son 1939, 1734 y 1082. La principal característica de este protocolo es que una vez que nos conectamos al servidor de correo, para ello debemos introducir nuestro usuario y contraseña, nos podemos descargar todos nuestros mensajes de correo a nuestro ordenador personal a través del gestor de correo electrónico que estemos utilizando, ya sea web o de escritorio.

El protocolo POP que actualmente se utiliza es POP3 que ha desbancado a los anteriores protocolos POP1 y POP2, ya que es muy superior a estos, aunque la mayoría de los clientes de correo son compatibles con los tres protocolos.

- **IMAP (Internet Mail Access Protocol)**

  Es el protocolo de acceso al correo electrónico a través de internet, es decir, es el protocolo que se utiliza para que nuestro cliente de correo se conecte al servidor y así tener acceso a nuestros mensajes. Este protocolo utiliza los puertos 143 y 220 de comunicación TCP/IP. Las RFCs en las que se indican las características de este protocolo son 1176, 1203, 1730 y 2060. El protocolo IMAP permite realizar búsquedas selectivas sobre nuestros mensajes alojados en el servidor de correo electrónico, permite la administración de carpetas de correo por el usuario en el servidor. Para realizar cualquiera de estas funciones es necesario haber introducido en el servidor nuestro usuario y contraseña a través de nuestro cliente de correo, es decir,

habernos identificado para que el servidor de correo nos de acceso a nuestros mensajes.

- **MIME (Multipurpose Internet Mail Extensions)**

  Es el protocolo de extensiones de correo de internet multipropósito, es decir, es el estándar o protocolo utilizado en la red para enviar mensajes a través de Internet en varias partes y con datos adjuntos que necesariamente tienen que ser caracteres ASCII de 7 bits, esto reduce mucho el tipo de mensajes que se pueden enviar a través de internet ya que se trata de un conjunto de caracteres muy reducido. Son los propios clientes y servidores de correo los que traducen automáticamente a formato MIME cuando se envía o recibe un correo. Las RFCs en las que se indican las características de este protocolo son 2045, 2046, 2047, 4288, 4289 y 2077.

  Si nos gusta trabajar con clientes de correo que se conecten al servidor a través del protocolo POP, sólo podremos descargar a nuestro equipo mensajes completos, aunque estos consten de múltiples partes. Sin embargo si nuestro cliente de correo se conecta al servidor a través del protocolo IMAP, podremos trabajar con cada parte del mensaje independientemente.

- **SSL (Secure Socket Layer) o TLS (Transport Layer Secure)**

  Respectivamente son el protocolo de capa de conexión segura y el protocolo de seguridad de la capa de transporte, aunque pueda creerse que se tratan de protocolos diferentes, en realidad no es así, ya que ambos ofrecen seguridad, a través de medios criptográficos, a las comunicaciones realizadas a través de cualquier red de

comunicación, el protocolo TLS sustituyó al protocolo SSL, ya que el protocolo SSL no se trataba de un protocolo debidamente estandarizado, pues fue desarrollado por Netscape en 1.996 para dar servicio a su navegador web, posteriormente se decidió estandarizar el protocolo SSL, para dar soporte a cualquier navegador web, y se decidió crear el protocolo TLS descrito en la RFC 2246 por primera vez en 1.999. Este protocolo interactúa con otros servicios de internet como HTTP, SMTP o NNTP, para ofrecer comunicaciones seguras, ya sea para realizar transacciones comerciales, envío de correo electrónico, consultar cuentas bancarias, etcétera. El protocolo proporciona autenticidad y privacidad en comunicaciones a través de internet para las aplicaciones cliente-servidor, mediante el uso de claves públicas para los clientes, el proceso de intercambio de claves está basado en certificados digitales y la comunicación recibe un proceso de cifrado simétrico para asegurar la confidencialidad de la información. Tanto el tipo de claves públicas como el tipo de cifrado simétrico no son siempre iguales para todas las comunicaciones, ya que antes de comenzar el envío de la información, el cliente y el servidor realizan un proceso de negociación, durante el cual se decide el tipo de clave pública y de cifrado simétrico a utilizar durante la comunicación.

3. SEGURIDAD INFORMÁTICA.

3.1 INTRODUCCIÓN.

A lo largo de este tercer punto hablaremos sobre la seguridad informática, ya que nuestro proyecto al tratarse de una auditoría en Lotus Notes, desde el punto de vista de la seguridad, hemos pensado que debíamos tratar el tema de la seguridad de la información y el tema de la seguridad informática, ya que son dos temas ampliamente relacionados con el contenido de presente proyecto final de carrera. Aunque es conveniente recalcar, que no entraremos en profundidad en ninguno de los apartados tratados a lo largo de este punto, ya que no todos los temas tratados aquí son implementados por Lotus Notes, y los que sí son implementados serán vistos en detalles más adelante.

Hemos creído necesario comentar los dos conceptos, en lugar de uno sólo, ya que dependiendo de a que expertos consultemos, tendremos la impresión de que se trata de dos conceptos distintos, aunque muy relacionados o que la seguridad informática es uno de los puntos de la seguridad de la información o ni siquiera eso.

Esperamos que con la inclusión de este punto en la memoria del presente proyecto final de carrera podamos solventar las dudas más generales de todas aquellas personas que no sean expertas ni en seguridad informática ni en la seguridad de la información, ya que entendemos que las personas expertas en dichas materias tienen unos conocimientos muy superiores a los que trataremos a lo largo de este proyecto final de carrera.

3.2 ¿QUÉ ES LA SEGURIDAD INFORMÁTICA?

En primer lugar trataremos de dar una definición de seguridad informática; pero como hemos comentado anteriormente no es posible entender el concepto de seguridad informática sin conocer el concepto de seguridad de la información. Por lo que daremos la siguiente definición de seguridad de la información.

Seguridad de la información:

Aunque pueda parecer que la seguridad de la información es un término relativamente moderno, tanto los conceptos, las herramientas y los mecanismos utilizados en el control de la seguridad de la información, están siendo utilizados por el ser humano desde hace muchos siglos. Ya que desde tiempos inmemoriales el ser humano ha sentido la necesidad de ocultar o proteger la información, ya fuera por temas militares, económicos o simplemente de intimidad.

A lo largo de los siglos la información ha pasado de ser un simple elemento de trabajo a convertirse en uno de los activos más importantes de las empresas u organizaciones, incluso hay organizaciones en las que su único activo es la información. Por este motivo es tan importante salvaguardar la información y poder asegurar su veracidad.

Por lo tanto, cualquier tipo de error o pérdida de información puede ser catastrófico para la organización e incluso puede ser la causa de la desaparición de dicha organización. Ya que esto puede suponer desde un desprestigio de la organización hasta graves pérdidas económicas para la misma.

A la vista de estas observaciones, podemos afirmar que en la actualidad para toda organización es de vital importancia asegurar la protección de su información y que por lo tanto, deberá haber al menos un departamento encargado de verificar que todos los requerimientos y estándares de la organización al respecto se cumplen escrupulosamente.

Si nos atenemos a la definición que se hace en el estándar ISO 27002, la seguridad de la información: "E*s la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales."*

La siguiente definición de seguridad de la información no ha sido recogida de ningún estándar ni libro especializado, pero hemos creído conveniente incluirla por su sencillez ya que creemos que es una definición que está al alcance de cualquier persona, esté relacionada o no con el mundo de la informática: *La seguridad de la información es toda medida, técnica o política empleadas por las organizaciones para asegurar que la información utilizada no ha sufrido ninguna modificación no autorizada.*

Seguridad informática:

Por contraposición con la seguridad de la información, el término de seguridad informática sí es un término moderno, ya que hace referencia a la seguridad en los sistemas informáticos y éstos hasta la segunda mitad del siglo XX no comenzaron a extenderse como sistemas de almacenamiento y procesamiento de información.

A continuación daremos una definición de seguridad de la información extraída del estándar ISO 27002, que creemos bastante acertada como definición de seguridad informática, ya que como hemos comentado anteriormente, es difícil separar ambos términos.

"La seguridad informática es la preservación de la confidencialidad, la integridad y la disponibilidad de la información, en cualquier circunstancia."

A continuación trataremos de dar una definición para tres conceptos que aparecen en la definición (en este caso las definiciones han sido tomadas directamente del estándar ISO 27001), para que la definición de seguridad de la información, quede más clara.

- **Confidencialidad**: *Asegura que únicamente el personal autorizado tenga acceso a la información*, es decir, sólo las personas a las que va destinada la información tienen acceso a la misma.
- **Disponibilidad**: *Cerciorar que los usuarios autorizados tendrán acceso a la información cuando la requieran y a sus medios asociados*, es decir, que la información únicamente es accesible por las personas autorizadas a tener acceso a la misma, en la forma que ellas quieran y en el momento que deseen.
- **Integridad**: *Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas; preservando exactitud y completitud de la misma y de los métodos de su procesamiento*, es decir, se asegura que la información es exacta y completa en todo momento, ya que sólo ha podido ser modificada por las personas autorizadas a ello.

3.3 PILARES DE LA SEGURIDAD INFORMÁTICA

En este punto enumeraremos los puntos que consideramos más importantes para los sistemas informáticos desde el punto de vista de su propia seguridad, por este motivo los hemos designado como pilares, ya que creemos que es en estos puntos en los que debemos basarnos para certificar o comprobar la seguridad de un sistema informático.

En este punto de la memoria todavía no realizaremos distinción alguna entre la seguridad física y la seguridad lógica, ya que consideramos que los pilares que describiremos a continuación son igualmente necesarios tanto para la seguridad lógica como para la física.

- **Control de privilegios.**

  Desde el punto de vista de la seguridad informática es importantísimo que cada perfil de usuario tenga claramente definidos sus privilegios de usuario sobre el sistema y que los usuarios no puedan realizar modificaciones sobre sus privilegios. Por lo que es de vital importancia crear mecanismos que aseguren que ninguno de los usuarios del sistema pueda realizar escaladas de privilegio, para obtener un acceso al sistema que no esté vinculado con su perfil de usuario y que por lo tanto no ha sido autorizado para obtener dichos accesos o privilegios.

- **Respaldo de la información alojada en el sistema.**

  Desde el punto de vista de la seguridad informática poder asegurar en todo momento que la información que se encuentra en los sistemas informáticos no se perderá ante un posible error humano o

del sistema es crítico, ya que actualmente la información es uno de los activos más importantes de cualquier organización. Por lo que es de vital importancia que se creen las políticas y mecanismos necesarios de copias de seguridad, para que no se pueda producir la pérdida de información. Dependiendo del tipo de negocio de la organización, bastará con tener copias de sólo una parte de la información o será necesario tener copias de la totalidad de la información que maneje la organización.

- **Redundancia del sistema.**

  Desde el punto de vista de la seguridad informática la redundancia de los sistemas es muy importante, ya que un sistema que no es redundante no asegura que sea accesible en todo momento por las personas autorizadas, esto choca con la definición de seguridad informática que hemos facilitado en el apartado anterior. Debido a esto, las distintas organizaciones han de desarrollar sistemas que permitan tener acceso siempre al sistema independientemente de las diferentes caídas del sistema, ya sea mediante duplicación de equipos, sistemas de alimentación ininterrumpida, distintas compañías de luz y adsl,…

- **Control de modificación de la información.**

  Para la seguridad informática es de vital importancia que sólo las personas autorizadas puedan modificar la información del sistema, en la forma y momento en los que están autorizados. Debido a este motivo, es necesario que las organizaciones describan políticas y diseñen los mecanismos necesarios para asegurar que únicamente el

personal autorizado pueda tener acceso a los datos para su modificación, es decir, que tengan usuarios sólo de conexión y visualización de datos, y tengan otros usuarios diferentes para poder modificar los datos de la organización. Ya que si no es así cualquier persona de la organización podría realizar modificaciones sobre los datos, que podrían llegar a ser funestas para la organización, ya fuera por desconocimiento del personal o por motivo de venganza con respecto a la organización.

- **Control de actualización.**

  Desde el punto de vista de la seguridad informática tener todos los sistemas informáticos debidamente actualizados, tanto en hardware como en software, es básico para el correcto funcionamiento de todos sus sistemas informáticos. Puesto que si alguno de los sistemas no está actualizado con el último software o hardware, es muy probable que los sistemas no funcionen correctamente, por lo que pueden producirse fallos y esto suele traducirse en un desprestigio para la organización o incluso pueden derivar en graves pérdidas económicas. Por lo tanto, la organización deberá crear las políticas y mecanismos necesarios para evitar que los sistemas informáticos puedan quedarse desactualizados.

- **Control de acceso.**

  Desde el punto de vista de la seguridad informática tener controlados los accesos que se realizan sobre los sistemas informáticos es vital, ya que si se produce algún fallo en el sistema, debido a manipulaciones humanas, tendremos registrado quién fue el último

usuario que se conectó al sistema y las modificaciones que realizó sobre el mismo. De esta manera, se podría intentar recuperar el sistema a su estado anterior deshaciendo los cambios realizados por el último usuario. Con esta medida podríamos minimizar los efectos causados por un usuario con poca experiencia o por un usuario mal intencionado, que intentase boicotear a la organización por motivos personales o económicos.

- **Relación coste/seguridad del sistema.**

  Es importante destacar este aspecto, ya que tanto para las organizaciones como para los expertos en seguridad informática, es un punto un tanto controvertido. Ya que según algunos expertos en seguridad informática, lo primero siempre es la seguridad, es decir, que no importa el coste en tiempo y dinero de un sistema informático para que éste sea todo lo seguro posible. Sin embargo, para las organizaciones lo más importante es la relación coste/seguridad informática, es decir, para las organizaciones no tiene sentido que el coste de mantener la seguridad informática del sistema sea más elevado, que el valor potencial para la organización de la información almacenada en los sistemas. En este caso, parece que el punto de vista más acertado es el segundo, pues no es racional que una organización, sea del tipo que sea, gastes más recursos económicos y humanos en proteger su información, que el valor de la propia información en sí misma.

- **Formación en seguridad informática del personal.**

  Desde el punto de vista de la seguridad informática, que todo el personal de la organización tenga al menos unas nociones básicas de seguridad informática es importantísimo, ya que de esta forma se consigue difundir entre el personal la importancia de la seguridad para la organización y que ésta no es nada mágico, sólo conocida por unos pocos iniciados. Para cumplir esta premisa, la organización deberá dar distintos cursos a sus empleados para adquirir los conocimientos necesarios. De esta forma, la organización conseguirá reducir de manera muy importante los errores humanos y los gastos derivados de dichos errores.

- **¿Qué proteger y de quién?**

  Para cualquier organización es fundamental tener claro que parte o partes de sus sistemas informáticos se desea proteger y de quién. Por lo que antes de tomar cualquier decisión o crear cualquier política o mecanismo de defensa, se han de tener claras estas dos premisas.
  Para ello se deberá crear en primer lugar un grupo de trabajo, formado por expertos en seguridad informática, que se encargará de crear un listado con las prioridades de la organización y otro listado con los diferentes tipos de ataque que pueda sufrir el sistema debido a la naturaleza de la organización y a la información almacenada en sus sistemas. Una vez que se tengan claras estas dos premisas se deberá pasar a crear las distintas políticas, procedimientos, mecanismos, cursos a impartir al personal,…

3.4 AMENAZAS, VULNERABILIDADES Y MEDIDAS DE PROTECCIÓN.

A lo largo de este punto trataremos de definir cuáles son los problemas más comunes de los sistemas informáticos y cuáles suelen ser las mejores medidas para solucionar dichos problemas.

Amenazas:

Según el estándar ISO 13335 la definición de amenaza es "*una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización."* Desde un punto de vista menos técnico, las amenazas que sufren los sistemas informáticos no son más que los tipos de ataque que pueden sufrir. Entendiendo como ataque, no la iteración directa de una persona mal intencionada, sino cualquier tipo de modificación sobre los parámetros del sistema en funcionamiento y su información, tanto a nivel de hardware como de software.

- Accidentales.

  Las amenazas accidentales son todas aquellas modificaciones sobre los parámetros del sistema que no se producen de forma voluntaria. Este tipo de amenazas vienen derivadas de los errores de los usuarios (tanto fallos de programación, fallos en la utilización del sistema,…), fallos hardware por desgaste de los materiales, caídas en los suministros de infraestructuras (corriente eléctrica, ADSL, fallos en el sistema de climatización,…)

- Naturales.

  Las amenazas naturales son todas aquellas modificaciones sobre los parámetros del sistema que se producen por lo que se denominan

causas de fuerza mayor. Este tipo de amenazas vienen derivadas por los accidentes o catástrofes naturales, como por ejemplo fuegos, inundaciones, terremotos,…

- Intencionadas

  Las amenazas intencionadas son todas aquellas modificaciones sobre los parámetros del sistema, especialmente sobre el software, que son realizadas con premeditación por terceras personas. En este tipo de amenazas podemos hacer distinción entre dos tipos:

  - **Pasivas:**

    Este tipo de amenazas se centran especialmente en la interceptación de las comunicaciones, para obtener los datos transferidos en ellas. Normalmente atentan contra la confidencialidad de las comunicaciones y por lo tanto de los datos transferidos en ellas. No modifican la información en ningún caso, pero si se hace con ella. Suelen ser difíciles de detectar.

  - **Activas:**

    Este tipo de amenazas se centran no en capturar la información, como en el caso anterior, sino que tratan de realizar modificaciones sobre la información, tanto almacenada en los sistemas como la información que se transfiere de un sistema informático a otro. Este tipo de amenaza es más fácil de detectar que las anteriores ya que se puede comprobar si la información ha sido modificada durante algún procesado de información o transferencia. Tras sufrir un ataque de este tipo, es posible

restaurar el sistema a su estado anterior. Algunos ejemplos de este tipo de ataque son: suplantación de identidad en transferencias de datos, interrupción de transferencias, modificación de hardware y software, secuestro de sesiones, borrados de datos,…

Vulnerabilidades:

Según el estándar ISO 13335 la definición de vulnerabilidad es "*la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas"*. Desde un punto de vista menos técnico las vulnerabilidades son los fallos que presentan los sistemas, y que por lo tanto pueden ser utilizados para llevar a cabo un ataque contra el sistema que dañe la seguridad del mismo o incluso que llegue a romperla por completo.

- Físicas:

  Todos los sistemas tienen múltiples vulnerabilidades físicas, estas básicamente consisten en aprovechar algún defecto de configuración del hardware o el software, que permita acceder a la información del sistema informático sin necesidad de haber iniciado sesión o incluso sin necesidad de arrancar el sistema. Algunas de estas vulnerabilidades son: que se permita arrancar el sistema desde cualquier soporte externo, que los datos del disco no estén cifrados, que el sistema no disponga de mecanismos de cierre de seguridad,… Algunos expertos en seguridad sostienen que si se tiene acceso físico al sistema, sólo es cuestión de tiempo encontrar una vulnerabilidad física y explotarla para tener acceso al sistema informático.

- Humanas:

  Este tipo de vulnerabilidades, como su propio nombre indica, vienen derivadas de la iteración del ser humano con los sistemas informáticos. Suelen deberse principalmente a usuarios inexpertos que no saben cómo configurar correctamente los sistemas, a malas elecciones de clave para el acceso a los sistemas, no actualizar debidamente el software de los equipos,…Aunque la mayoría de las vulnerabilidades de este tipo vienen derivadas de los despistes de los usuarios o de su negligencia, dentro de este tipo de vulnerabilidades también se incluyen aquellas modificaciones en la configuración de los sistemas por parte de usuarios mal intencionados, con el fin de aprovecharse de dicha vulnerabilidad en el futuro.

- Comunicaciones:

  Este tipo de vulnerabilidades vienen derivadas de la alta complejidad de las redes de comunicación. Suelen estar producidas por la escasez de recursos humanos en la administración de las redes de comunicación, es decir, suele haber un volumen muy grande o de puntos de acceso o de sistemas conectados en relación con el número de personas encargadas de la administración. Aunque también puede ser debido a la necesidad de realizar múltiples reconfiguraciones de los sistemas de comunicación en un corto espacio de tiempo, por necesidades de los diferentes sistemas de información que se encuentren en la red. Debido a esto, es bastante probable que se pueda encontrar una vulnerabilidad en las comunicaciones durante

una ventana de tiempo considerable y que pueda ser aprovechada para obtener acceso al sistema informático.

Ahora procederemos a describir el perfil de las personas que suelen aprovechar los distintos tipos de vulnerabilidades en los sistemas informáticos para llevar a cabo ataques sobre los mismos, teniendo en cuenta si tienen algún tipo de relación con la organización propietaria de los sistemas:

- PERSONAS INTERNAS:

  Aunque a priori pueda parecer contradictorio, la mayoría de ataques efectivos que sufren los sistemas informáticos son producidos por empleados o ex-empleados de la organización que conocen perfectamente las vulnerabilidades del sistema y se benefician de este conocimiento para obtener accesos ilícitos a los sistemas informáticos de la organización. Este acceso puede deberse desde a conocer los datos de acceso al sistema de otro usuario hasta crear una vulnerabilidad a medida en el sistema informático para utilizarla con posterioridad.

  Este tipo de ataques suelen ser llevados a cabo por personal descontento con el trato que se le ha dado en la organización y tienen como finalidad principal la pérdida de credibilidad y el deterioro de la imagen corporativa de la organización, con las consecuentes pérdidas económicas de dicho descrédito; aunque también suelen buscar un enriquecimiento personal a costa de la organización. En el primer caso lo que se busca es un ataque que tenga mucha repercusión, es decir, denegación de servicios por parte de los sistemas informáticos de la organización, con lo que se dejará de

ofrecer alguno o varios de los servicios facilitados por la organización. Mientras que en el segundo caso lo que se busca es un ataque transparente para la organización, es decir, que pase desapercibido y nadie dentro de la organización pueda detectarlo, para que de esta forma el atacante pueda lucrarse de sus actos sin temor a ninguna consecuencia.

- PERSONAS EXTERNAS:

  Este tipo de ataques suelen ser llevados a cabo por personas completamente ajenas a la organización, aunque en este caso la finalidad de dichos ataques puede ser ligeramente diferente, ya que aunque los motivos de los ataques pueden ser los mismos que en el caso anterior, también cabe la posibilidad de que el único motivo para realizar el ataque sobre el sistema sea el ego personal, el reconocimiento por parte de otros atacantes, o simplemente por diversión. Estos ataques son mucho más elaborados y trabajosos por parte de los asaltantes que los del punto anterior, ya que no conocen la estructura interna ni del sistema ni de la organización, por lo que requieren una primera fase de análisis del estado del sistema informática, una fase de estudio de las vulnerabilidades encontradas y por último una planificación de cómo llevar a cabo el ataque al sistema informático.

Medidas de protección:

Las medidas de protección sobre los sistemas informáticos son todas aquellas decisiones que se toman para mejorar la seguridad del sistema, teniendo en cuenta las vulnerabilidades del sistema.

Hay que tener en cuenta que antes de implantar cualquier tipo de medida deberá haberse realizado un estudio detallado sobre los beneficios de dicha medida y del coste real de su implantación, tanto el coste económico como el coste en horas de trabajo.

A continuación procederemos a describir los distintos tipos de medidas que las organizaciones pueden tomar para hacer frente a los ataques sobre sus sistemas informáticos.

- Forma de actuar de la medida contra la vulnerabilidad.

  -Preventivas: Este tipo de medidas se basan en realizar estudios pormenorizados del sistema informático y hallar las posibles vulnerabilidades del mismo y tratar de subsanarlas.

  -De detección: Este tipo de medidas se basan en la creación de sistemas que sean capaces de detectar cualquier tipo de ataque contra el sistema, ya sea por un control exhaustivo en los datos almacenados en los sistemas, o por un control de las conexiones a los sistemas.

  -De corrección: Este tipo de medidas se llevan a cabo tras un ataque, y se limitan únicamente a estudiar el ataque y a subsanar la vulnerabilidad de la que se aprovecharon los atacantes, para que no se produzcan de nuevo ataques aprovechando vulnerabilidades ya conocidas.

  -De recuperación: Este tipo de medidas, al igual que la anterior, se llevan a cabo tras un ataque, y su función es volver a dejar el sistema informático exactamente igual a antes del ataque, es decir, estas

medidas se utilizan para que en caso de que se produzca un ataque no se pierda ninguno de los datos almacenados en los sistemas.

- Según la naturaleza de la medida.

  -Físicas: Este tipo de medidas se basa en proteger el acceso físico al sistema y su entorno, es decir, limitan el acceso a personas a la sala en la que se encuentran los sistemas informáticos y el acceso a los propios sistemas informáticos. Se suelen implementar mediante dispositivos hardware, que suelen ser de un coste moderado y de fácil implantación.

  -Técnicas: Este tipo de medidas pretenden tanto proteger el software como el hardware, por lo que su implementación se realiza como herramientas de software y hardware. Para llevar a cabo estas medidas es necesario que las personas que las implanten tengan una gran formación técnica en materias como criptografía, bases de datos, sistemas operativos, comunicaciones,…

  -Administrativas y organizativas: Este tipo de medidas se basan en la creación de políticas y procedimientos a seguir por todos los trabajadores de la organización, ya que si las cosas están correctamente planificadas desde el principio, será más difícil que queden cabos sueltos, para que sean aprovechados por atacantes para obtener acceso al sistema. Básicamente en ellas se definen responsabilidades y tareas, se crean departamentos u organismos para el seguimiento de incidencias, se crean planes de contingencia y auditorías tanto internas como externas.

-Legales: Este tipo de medidas no son implementadas por la organización a la que pertenecen los sistemas de información, sino que son implementadas por los estados. Las organizaciones están obligadas a cumplir estas medidas legales, ya que su incumplimiento les puede suponer desde una sanción económica importante hasta el cierre de la organización o que alguno de los miembros de la organización se vea obligado a entrar en prisión. Las medidas de este tipo suelen quedar recogidas en la legislación vigente de los distintos países.

3.5 CRIPTOGRAFÍA.

Hemos decidido incluir este punto en la memoria de nuestro proyecto fin de carrera, debido a la gran importancia que tiene la criptografía dentro de la seguridad informática, ya que muchos de los puntos tratados anteriormente, no se pueden entender sin la criptografía. La criptografía bien aplicada puede asegurar la integridad, la confidencialidad de la información y prevenir su repudio, que como hemos visto anteriormente son puntos fundamentales para asegurar la seguridad de los sistemas informáticos.

A lo largo de este punto trataremos de dar una definición, que creemos acertada, de criptografía, explicaremos algunos conceptos básicos relacionados con la criptografía y hablaremos sobre los distintos tipos de cifrado y de los distintos tipos de criptoanálisis.

Utilizando la definición que hace Jorge Ramió Aguirre en su libro "Seguridad Informática y Criptografía" la criptografía es: "*una rama inicial de las matemáticas y en la actualidad de la informática y la telemática que hace uso de métodos y herramientas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo y una o más claves, dando lugar a distintos criptosistemas que permiten asegurar, al menos, dos aspectos básicos de la seguridad como son la confidencialidad y la integridad de la información.*"

En este pequeño esquema se trata de mostrar el proceso de ocultación de la información.

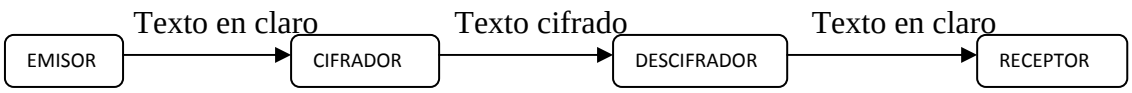

Figura 3.1: Ejemplo del proceso de ocultación de la información.

EMISOR: Es quien genera el mensaje.

RECEPTOR: Es a quien va dirigido el mensaje.

CIFRAR: Es el proceso de encubrir la información.

DESCIFRAR: Es el proceso inverso a cifrar.

Tipos de cifrado:

A continuación procederemos a agrupar los distintos tipos de cifrado según sus características.

- Naturaleza: Esta clasificación se hace teniendo en cuenta la naturaleza del criptograma utilizado para cifrar, es decir, si se sustituyen siempre unos datos por otros, o según la posición que ocupen, o si se permutan unos datos por otros. Respectivamente se nombran como sustitución, producto y transposición.
- Clave utilizada: Esta clasificación se hace teniendo en cuenta si la clave utilizada para cifrar y descifrar es la misma o no. Respectivamente se nombran como simétricos y asimétricos.
- Número de símbolos cifrados: Esta clasificación se hace teniendo en cuenta el número de símbolos cifrados con cada clave, es decir, si para cada clave se cifra un único símbolo o se cifran varios. Respectivamente se nombran como de flujo y de bloque.

Métodos criptográficos clásicos:

- Sustitución simple mono alfabeto: Se basa en la sustitución de un carácter por otro mediante la utilización del siguiente algoritmo:

  $$E(i) = a_i + b \pmod n$$

  Siendo **i:** la posición del carácter dentro del mensaje, **E:** la función de cifrado, **b:** constante de desplazamiento, **a:** constante de decimación, **n:** número de caracteres del alfabeto utilizado, **a** y **n** no deben tener divisores comunes y **a** y **b** son las clave utilizadas.

- Sustitución poli alfabética: Se basa en la sustitución simple aplicada de manera periódica con periodo **d**, que son los métodos de sustitución simple utilizados, es decir, para cada parte del mensaje se utiliza un cifrado simple independiente con la periodicidad determinada por **d**. Dentro de esta categoría podemos incluir tres tipos de cifrado, el cifrado Vigenére, el cifrado de clave continua y el cifrado con autoclave.

  El cifrado Vigenére se basa en tomar como clave una palabra sencilla de recordar y cifrar con esa palabra todo el mensaje mediante sustitución poli alfabética.

  El cifrado de clave continua se basa en tomar un texto conocido por el emisor y el receptor del mensaje, y con ese texto cifrar todo el mensaje mediante sustitución poli alfabética.

  El cifrado con autoclave se basa en tomar una palabra sencilla y el propio texto del mensaje y concatenarlos para realizar un cifrado de sustitución poli alfabética.

- Máquinas de cifrado: Las máquinas de cifrado son instrumentos que se han utilizado durante años, para cifrar la información. Desde los tiempos de los persas hasta la actualidad han sido utilizadas para facilitar el cifrado al ser humano. Básicamente consisten en una estructura interna mecánica que aplica diferentes métodos de cifrado alternativamente y de forma secuencial.
- Cifrado tipo Vermam: En la actualidad es considerado el método de cifrado más seguro, ya que toda su fuerza reside únicamente en la seguridad de la clave, por lo que si se utiliza una clave aleatoria e infinita, es imposible descifrar el mensaje sin ella. Consiste en la utilización de la función lógica xor para cifrar la información, es decir, se aplica la siguiente ecuación para cifrar toda la información

  $\mathbf{C=M \oplus K}$
- Sustitución poligráfica: Se basa en la utilización de matrices para realizar el cifrado de la información, es decir, se agrupan los caracteres en forma de matriz, se elige una clave con forma de matriz y que tenga inversa, para poder utilizarla en el proceso de descifrado, y se multiplican ambas matrices para obtener el mensaje cifrado.

Tipos de criptoanálisis:

El criptoanálisis se encarga de estudiar los métodos de descifrado, y se basa en que la seguridad de un cifrado debe recaer única y exclusivamente en la clave y no en el algoritmo utilizado para cifrar, es decir, que la seguridad del cifrado dependa exclusivamente de conocer la clave que se utilizó para realizar

el cifrado. Los criptoanalistas buscan la manera de conseguir la clave de cifrado o de conseguir la información original.

A continuación procederemos a enumerar los principales tipos de criptoanálisis:

- Al criptograma: Este tipo de criptoanálisis se centra en intentar obtener la información descifrada, partiendo de la información cifrada y conociendo el algoritmo de cifrado, mediante la utilización de análisis estadístico y la utilización de distintas claves.
- Al texto en claro conocido: Este tipo de criptoanálisis se centra en tratar de averiguar la clave de cifrado, conociendo tanto el algoritmo de cifrado, como la información cifrada y sin cifrar.
- Al texto en claro escogido: Este tipo de criptoanálisis se centra en intentar obtener la clave de cifrado partiendo de una información descifrada elegida y conociendo el método de cifrado y la información cifrada.
- Al texto cifrado elegido: Este tipo de criptoanálisis se centra en intentar obtener la clave partiendo de la información cifrada, que para este proceso es descifrada, y se estudia para intentar obtener características de la información cifrada y descifrada que permitan obtener la clave de cifrado.

Criptografía de clave pública:

Este tipo de criptografía utiliza cifrados de clave asimétrica, la clave que se utiliza para cifrar la información es pública, es decir, es conocida por todo el mundo, en cambio la clave utilizada para descifrar la información es conocida

sólo por el emisor y el receptor del mensaje, aunque cada uno de ellos tienen una pareja de claves distintas, pero ambas parejas son equivalentes.

Para asegurar la privacidad de las claves se utiliza una función irreversible, es decir, se utiliza una función de una complejidad muy baja para calcular los mensajes cifrados y descifrados, pero que realizar el proceso inverso es extremadamente complejo, es casi imposible obtener las claves partiendo del mensaje cifrado. Esta función es del tipo $\mathbf{y= g^x (mod\ p)}$, y su inversa sería $\mathbf{x=\log_g (y)(mod\ p)}$, y realizar este último cálculo es computacionalmente inabarcable.

Normalmente el receptor del mensaje y el emisor acuerdan la clave entre los dos, escogen un número primo (p) de más de 200 dígitos y una raíz primitiva de ese número (g) y escogen cada uno un número muy grande menor que p-1, y envían respectivamente al otro $\mathbf{X=g^x\ mod\ p}$ y $\mathbf{Y=g^y mod\ p}$, cada uno de ellos calculan respectivamente $\mathbf{Y^x =g^{yx}\ modp}$ y $\mathbf{X^y = g^{yx}\ mod\ p}$, y de esta manera queda acordada la clave $\mathbf{K=Y^x=X^y}$.

Criptografía de clave privada:

Este tipo de criptografía utiliza cifrados de clave simétrica, la clave que se utiliza para cifrar la información es privada, es decir, es conocida sólo por el emisor y el receptor del mensaje. Para realizar el cifrado se utilizan una serie de transformaciones no lineales sobre los datos originales.

La seguridad del cifrado recae única y exclusivamente en la clave de cifrado/descifrado. Debido a la no linealidad de los algoritmos de cifrado, en teoría el único ataque posible sobre el cifrado sería por fuerza bruta, es decir, se deberían probar todas las posibles claves para intentar obtener los datos originales.

A continuación procederemos a describir de forma genérica el algoritmo de cifrado AES que es el criptosistema de clave privada más importante y utilizado en la actualidad, por eso hemos decidido incluir esta pequeña descripción del mismo.

Las principales características de AES son que utiliza claves de tamaño variables de 128, 192 y 256 bits, aunque también puede utilizar claves con tamaño múltiplos de 4 bytes. Usa un cifrado de bloque de 128 bits o múltiplos de 4 bytes. Usa operaciones modulares a nivel de byte y de palabras de 32 bits. Tiene un número de etapas flexibles, por lo que no en todos los cifrados se usan el mismo número de etapas. Todas las operaciones que se realizan son a nivel de byte.

Utiliza un conjunto de operaciones unidireccionales y no lineales, mediante las cuales se realizan distintas permutaciones secuenciales en varias pasadas, estas operaciones forman lo que se denomina Caja S del algoritmo, dentro de las cuales radica la fortaleza del algoritmo. Esta Caja S, está formada por tres capas, una primera capa conocida como Capa de Mezcla Lineal, en la que se realiza una difusión de la información a nivel de bit. Una segunda conocida como Capa No Lineal, en la que se realizan una serie de permutaciones de forma secuencial y en varias rondas. Y por último la Capa Clave, en la que se realizan operaciones xor con las subclaves y la información de esta etapa determinada.

Las transformaciones que se realizan en cada uno de los pasos del algoritmo se denominan estados. Se representan por una matriz de 4 filas y 4 columnas para el texto en claro y de 4 filas y 4, 6 u 8 columnas para las claves.

Como se puede ver hasta aquí el cifrado AES no es trivial ni fácil de explicar, pero teniendo en cuenta la naturaleza de nuestro proyecto, no creemos necesario entrar a definir más en profundidad el algoritmo, pues nuestra idea era dar una visión general del mismo y no una explicación exhaustiva de su funcionamiento.

3.6 FIRMA DIGITAL.

Según el estándar ISO 7498-2 la firma electrónica se puede definir como "*conjunto de datos, o transformación de datos, que permiten al receptor de los mismos probar el origen y la integridad de los datos recibidos, así como protegerlos contra falsificaciones*".

La firma digital permite autentificar de forma unívoca al remitente de cualquier información propietario de la firma electrónica con la que dicha información está firmada, garantiza la integridad de la información contenida en el mensaje recibido y en el supuesto que se produzca algún tipo de contingencia legal puede utilizarse para solventar dicha contingencia.

La firma digital ha de ser fácil de reproducir por su propietario, el propietario de la firma no ha de poder rechazar su autoría, ha de ser única para que sólo su propietario pueda generarla y ha de ser fácilmente reconocible tanto por su propietario como por los posibles receptores de la información a la que acompaña la firma digital.

En función del tipo de clave y de la forma de intercambio de las claves existen varios tipos de firma digital, aunque todos cumples las condiciones comentadas anteriormente. Hemos decidido no explicar en detalle ninguno de los diferentes tipos de firma digital, porque no es motivo de estudio en el presente proyecto final de carrera y la inclusión de este punto en la memoria únicamente tiene como finalidad dar una visión general del concepto de firma digital, para que cualquier lector que no esté familiarizado con el término pueda entender su significado.

3.7 POLÍTICAS DE SEGURIDAD.

Las políticas de seguridad son el conjunto de principios y reglas generales que regulan la forma de proteger la información de una organización en todas las fases de su tratamiento.

Factores a considerar:

En primer lugar se debe decidir si únicamente afectará a un área, a varias o a toda la organización.

Habrá que intentar implicar no sólo a los responsables de la sección para la que se crea la política, sino también a todos los responsables de la organización. Ya que de esta forma se podrá tener un mejor conocimiento del estado del sistema, puesto que las decisiones que se tomen pueden afectar a toda el sistema informático de la organización.

Hay que tener en cuenta las relaciones con el resto de planes y políticas de las secciones de la organización. La política de seguridad debe estar integrada con estos planes, ya que puede afectar a los mismos.

Es necesario que se delimite el ámbito de aplicación y el personal de la organización afectado.

Aspectos a tratar:

-Organizativos. Hay que tener en cuenta a los responsables, tareas y líneas de dependencia de las distintas áreas de la organización. Crear una estructura departamental, así como elegir al responsable para coordinar y controlar la seguridad informática de la organización.

-De personal. Pueden ser el mayor escoyo para la aplicación de la política. Habrá que establecer sanciones administrativas para el personal de la organización, que traten de asegurar el cumplimiento de las políticas. Será

necesario que los empleados estén formados en seguridad para tratar de evitar errores y negligencias.

-De procedimiento. Las políticas de seguridad deben ser tenidas en cuenta tanto en el desarrollo de aplicaciones como en la adquisición, instalación y mantenimiento de sistemas informáticos. También deben ser tenidas en cuenta en la gestión, mantenimiento y cambios de los distintos sistemas informáticos de la organización.

-Clasificación de la información. Habrá que tener en cuenta la importancia y sensibilidad de la información para la organización y las posibles repercusiones legales que puedan producirse por un mal uso de esa información. Distinguir las informaciones más importantes del resto y saber cómo se deben manejar y proteger. Hacer un balance entre el valor de la información y las complejidades administrativas que impone dicha clasificación.

-Gestión de incidencias. Habrá que tener en cuenta que es necesario crear un registro de incidencias, que permita mantener un histórico de incidencias para realizar estadísticas de incidencias y previsiones de futuras incidencias.

-Análisis y gestión de riesgos. Siempre se deberá incluir la previsión más negativa respecto a los riesgos, es decir, habrá que incluir el peor escenario posible.

-Plan de contingencia. Es la definición de las acciones a realizar, los recursos a utilizar y el personal a emplear en caso de producirse un acontecimiento que inutilice o degrade los recursos informáticos de la organización.

-Auditoría. Será necesario realizar auditorías tanto internas como externas periódicamente, para que verifiquen el cumplimiento de las políticas. Tras su realización se deberán analizar los resultados de las mismas, realizar las modificaciones recomendadas y realizar los controles recomendados.

4. LEGISLACIÓN VIGENTE Y ESTÁNDARES.

4.1 INTRODUCCIÓN.

Hemos creído conveniente incluir este punto porque creemos que es de vital importancia que conozcamos el marco legislativo en el que cualquier organización que opere en España, ya sea de forma directa o indirecta, deberá respetar y tratar de hacer cumplir por todos sus empleados. Así como a la organización internacional que promulgo la distintas medidas, políticas y estándares por las que se rigen la mayoría de entidades dedicas a las labores de seguridad de la información

A lo largo de este punto hablaremos sobre el marco jurídico-legal vigente en España para el tema que nos ocupa, es decir, la seguridad de la información, y sobre la entidad de estandarización más importante, en el tema de la auditoría informática, conocida como ISACA. Es conveniente destacar que la legislación de la que hablaremos a lo largo de este punto no es la única, sino la que hemos considerado más importante, hay que destacar que en el código penal español también se hace referencia a los Sistemas de Información, aunque a lo largo de este punto no se haga ninguna mención al tema, ya que no hemos creído necesario incluirlo en el presente proyecto final de carrera, puesto que creemos que hubiera sido un tanto excesivo hablar del mismo en un proyecto de seguridad informática y que por lo tanto no se centra en el tema legal.

A lo largo de este punto trataremos de dar una visión global de las distintas leyes dedicadas a la seguridad de la información y que sea fácilmente

entendible por cualquier persona, por lo que trataremos de evitar en la medida de lo posible la jerga jurídica, para hacer más llevadera la lectura de este punto.

4.2 LOPD

A lo largo de este apartado daremos una definición de esta ley, y enumeraremos los puntos de la misma, que nos parecen no más importantes, sino que consideramos más relevantes en relación al tema tratado en el presente proyecto final de carrera.

La Ley Orgánica del 15 de diciembre de 1.999 sobre Protección de Datos de Carácter Personal tiene como objetivo garantizar y proteger, en lo referente al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas.

A continuación procederemos a describir los principales aspectos de esta ley.

Disposiciones Generales.

Se aplica sobre los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados.

Rige todos los tratamientos de datos de carácter personal que se efectúan en territorio español, aquellos cuyo responsable aún no estando establecido en territorio español le sea aplicable la legislación española y a aquellos tratamientos de datos cuyo responsable no estando establecido en la Unión Europea utilice medios para el tratamiento de datos establecidos en territorio español.

El régimen de protección de datos descrito no es de aplicación para todos los ficheros mantenidos por personas físicas para uso de carácter exclusivamente personal o doméstico, todo fichero sometido a la normativa

sobre protección de materiales clasificados y todos los ficheros para la investigación del terrorismo y de formas graves de delincuencia organizada.

Rige todos los tratamientos de datos personales de los ficheros regulados por la legislación de régimen electoral, todos los ficheros que sirvan a fines exclusivamente estadísticos, los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación que se refiere a la legislación del régimen del personal de las Fuerzas Armadas, los derivados del registro civil y del registro central de penados y rebeldes y los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las fuerzas y cuerpos de seguridad.

A continuación mostraremos algunas definiciones hechas en el reglamento de esta ley, para que de esta forma quede más claro, si cabe, las condiciones de aplicación de la ley.

Accesos autorizados: *autorizaciones concedidas a un usuario para la utilización de los diversos recursos.*

Afectado o interesado: *persona física titular de los datos que sean objeto del tratamiento.*

Autenticación: *procedimiento de comprobación de la identidad de un usuario.*

Cancelación: *procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales.*

Cesión o comunicación de datos: *tratamiento de datos que supone su revelación a una persona distinta del interesado.*

Consentimiento del interesado: *toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.*

Contraseña: *información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.*

Control de acceso: *mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.*

Copia de respaldo: *copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.*

Dato de carácter personal: *toda aquella información concerniente a personas físicas identificadas o identificables*.

Destinatario o cesionario: *la persona física o jurídica pública o privada u órgano administrativo, al que se revelen los datos.*

Dato disociado: *aquél que no permite la identificación de un afectado o interesado.*

Encargado del tratamiento: *la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.*

Fichero: *todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.*

Fuentes accesibles al público: *aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.*

Identificación: *procedimiento de reconocimiento de la identidad de un usuario.*

Incidencia: *cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.*

Perfil de usuario: *accesos autorizados a un grupo de accesos.*

Procedimiento de disociación: *todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.*

Recursos: *cualquier parte componente de un sistema de información.*

Responsable del fichero o tratamiento: *persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.*

Responsable de seguridad: *persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.*

Sistema de información: *conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.*

Soporte: *objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.*

Transmisión de documentos: *cualquier traslado, comunicación, envío, divulgación o entrega de la información contenida en el mismo.*

Tratamiento de datos: *operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*

Usuario: *sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.*

Principios de Protección de Datos.

Los datos de carácter personal sólo se pueden recoger para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Los datos no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. Los datos serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

Si los datos registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados.

Los datos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad por la cual hubieran sido recabados o registrados.

Los datos serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

El tratamiento de los datos requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. No será preciso el consentimiento cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.

En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos que revelen la ideología, afiliación sindical, religión y creencias.

Los datos que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración,

pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

Los datos objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Será nulo el consentimiento para la comunicación de los datos a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter revocable.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del futuro tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Derechos de Acceso, Rectificación, Cancelación y Oposición.

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos que ofrezca una definición de sus características o personalidad.

La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las administraciones públicas.

En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Obligaciones previas al tratamiento de los datos.

Las distintas modificaciones que se hagan sobre los ficheros de protección de datos de las administraciones públicas, sólo se podrán hacer mediante disposición general publicada en el boletín oficial del estado o diario oficial correspondiente.

En el caso de la eliminación de los ficheros, se debe establecer el destino de los mismos o las medidas adoptadas para su destrucción.

Los ficheros que contengan datos de carácter personal, que hayan sido recogidos con finalidad administrativa, no podrán ser compartidos o suministrados a las distintas administraciones pública o los cuerpos de seguridad del estado, si han sido recogidos con cualquier otra finalidad, ya sea fiscal, procesal, etcétera, si pueden ser compartidos por los distintos cuerpos del estado, para facilitar cualquier tipo de tramitación del estado.

Para el caso de las organizaciones privadas, antes de realizar cualquier tipo de modificación sobre un fichero que contenga datos de carácter personal, deben realizar la notificación pertinente a la agencia española de protección de datos y está ha de dar su consentimiento para que dichas operaciones se puedan llevar a cabo. Aunque cabe destacar que para ciertas modificaciones del tipo cambio de domicilio, estado civil,… no es necesario esperar la autorización de la agencia española de protección de datos.

Si se decide traspasar la titularidad de un fichero que contenga datos de carácter personal también es necesario notificarlo a la agencia española de protección de datos, y también dicha agencia debe dar su consentimiento, también es obligatorio que realicen la notificación del cambio de titularidad a todas las personas afectadas con el cambio, es decir, todas aquellas personas y organizaciones que aparecen en dicho fichero.

Transferencias Internacionales de Datos.

No podrán realizarse transferencias temporales ni definitivas de datos que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

La parte de sanciones, infracciones y prescripciones no ha sido incluida ni en este apartado ni en ningún otro del actual proyecto final de carrera, ya que no se ha considerado importante su inclusión, puesto que la finalidad del actual proyecto no es que las personas que puedan leerlo se conviertan en unos expertos en la ley de protección de datos, sino que tengan unos conocimientos mínimos del espíritu de la ley, y que gracias a ello, puedan comprender cuales son los derechos y obligaciones tanto de las personas u organizaciones incluidas en los ficheros con datos de carácter personal como de las entidades propietarias de dichos ficheros, no así, cuales son las medidas o acciones legales que pueden acarrear el incumplimiento de la ley total o parcialmente.

Códigos tipo.

Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Los códigos tipo tendrán carácter voluntario.

Las administraciones públicas y las corporaciones de derecho público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.

Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la agencia española de protección de datos.

De las medidas de seguridad en el tratamiento de datos de carácter personal.

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este punto, con independencia de cuál sea su sistema de tratamiento.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

A los efectos de facilitar el cumplimiento de lo dispuesto en este punto, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas

Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados.

En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Cuando deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Procedimientos tramitados por la Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.

Se rige por lo dispuesto en la presente Ley Orgánica de Protección de Datos 15 de diciembre de 1.999 y por el Real Decreto 1665/2008 del 17 de Octubre que modifica al anterior Estatuto en el que se definían las responsabilidades de la agencia.

En el ejercicio de sus funciones públicas, actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

La Agencia Española de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

- Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
- Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
- Cualesquiera otros que legalmente puedan serle atribuidos.

La Agencia Española de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

La Agencia Española de Protección de Datos debe velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos, emitir las autorizaciones

previstas en la LOPD o en sus disposiciones reglamentarias, atender las peticiones y reclamaciones formuladas por las personas afectadas, proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal, requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la LOPD, informar de los proyectos de disposiciones generales, velar por la publicidad de la existencia de los ficheros de datos con carácter personal y cuantas otras le sean atribuidas por normas legales o reglamentarias.

Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados.

La publicación se realizará preferentemente a través de medios informáticos o telemáticos.

4.3 LSSI.

La Ley 34 de Julio de 2.002 de servicios de la sociedad de la información y de comercio electrónico tiene como objetivo incorporar a la legislación española la directiva europea 2000/31/CE de Junio del mismo año.

En esta directiva europea se trata de definir el concepto de sociedad de la información, ya que debido al gran crecimiento de las redes de telecomunicación y especialmente de internet se estaba empezando a producir un gran vacío legal que podría ser aprovechado por personas malintencionadas para realizar cualquier tipo de actividad lucrativa y poco transparente, por lo que era necesario crear un marco jurídico que se encargara de definir todos los posibles actores y sus funciones dentro de este nuevo medio.

Esta nueva ley contempla la contratación de bienes y servicios por vía electrónica, el suministro del medio, las actividades de intermediación relativas al suministro y acceso a la red, la transmisión de datos por medios electrónicos, la realización de copia temporal de las páginas de internet solicitadas por los usuarios, el alojamiento en los servidores de información, servicios o aplicaciones por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de internet, así como cualquier otro servicio que se preste a petición individual del usuario siempre que represente una actividad económica para el prestador.

Obviamente estos servicios son prestados por las distintas empresas dedicadas al sector de las telecomunicaciones.

Por lo tanto, esta ley se aplica a los prestadores de los distintos servicios establecidos en el ámbito nacional. Por establecimiento se entiende el lugar desde el que se dirige y gestiona una actividad económica.

Aunque la ley es igualmente aplicable a quienes sin residir en España prestan servicios de la sociedad de la información a través de un establecimiento permanente en España.

El lugar de establecimiento del prestador de servicios de la sociedad de la información determina la ley y las autoridades competentes para el control de su cumplimiento, de acuerdo con el principio de aplicación de la ley del país de origen que inspira la Directiva 2000/31/CE.

También recoge la anotación de nombres de dominios de internet que correspondan al prestador de servicios en el registro público en el que conste inscrito para la adquisición de personalidad jurídica, con el fin de garantizar la vinculación entre el prestador, el establecimiento físico y su localización en la red, para que sea fácilmente accesible para los usuarios y para la administración pública.

La ley establece las obligaciones y responsabilidades de los prestadores de servicios que realizan actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red.

Se impone a dichos prestadores un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando.

Las implicaciones que pueden derivar del incumplimiento de estas normas son de tipo civil o penal, en función de los bienes jurídicos afectados y las normas que resulten aplicables.

La ley impone a los prestadores de servicios la obligación de facilitar el acceso a sus datos de identificación a cuantos visiten su sitio en internet, informar a los destinatarios sobre los precios que apliquen a sus servicios y la

de permitir a éstos visualizar, imprimir y archivar las condiciones generales a que se someta, en su caso, el contrato.

Si la contratación se efectúa con consumidores el prestador deberá guiarles durante el proceso de contratación, indicándoles los pagos que han de hacer y la forma de corregir posibles errores en la introducción de datos, y confirmar la aceptación realizada una vez recibida.

La ley permite la realización de contratos por vía electrónica confiriéndoles el mismo valor a cualquier otro contrato en papel.

Las disposiciones contenidas en esta Ley sobre aspectos generales de contratación electrónica, como las relativas a validez y eficacia de los contratos electrónicos o al momento de prestación del consentimiento serán de aplicación aún cuando ninguna de las partes tenga la condición de prestador o destinatario de servicios de la sociedad de la información.

La ley promueve la elaboración de códigos de conducta sobre las materias reguladas en la misma, al considerar que son un instrumento de autorregulación especialmente apto para adaptar los diversos preceptos de la ley a las características específicas de cada sector.

Se potencia el recurso al arbitraje y a los procedimientos alternativos de resolución de conflictos que puedan crearse mediante códigos de conducta, para dirimir las disputas que puedan surgir en la contratación electrónica y en el uso de los demás servicios de la sociedad de la información.

Se favorece el uso de medios electrónicos en la tramitación de dichos procedimientos, respetando las normas que establezca la normativa específica sobre arbitraje.

Se regula la acción de cesación que podrá ejercitarse para hacer cesar la realización de conductas contrarias a la presente ley que vulneren los intereses de los consumidores y usuarios.

Se prevé la posibilidad de que los ciudadanos y entidades se dirijan a diferentes Ministerios y órganos administrativos para obtener información práctica sobre distintos aspectos relacionados con las materias objeto de esta ley, lo que requerirá el establecimiento de mecanismos que aseguren la máxima coordinación entre ellos y la homogeneidad y coherencia de la información suministrada a los usuarios.

Asimismo se contemplan una serie de revisiones orientadas a hacer efectiva la accesibilidad de las personas con discapacidad a la información suministrada por los medios electrónicos, y muy especialmente a la información suministrada por las administraciones públicas.

No hemos creído necesario entrar en más detalle, ya que al igual que nos sucedía en el apartado 4.2 del presente proyecto final de carrera, la finalidad de este proyecto no es que las personas que lo lean se hagan expertos en la legislación aplicable a los sistemas de información, sino que gracias a la lectura del mismo puedan tener una visión global, aunque no completa, del marco jurídico aplicable a los usuarios y propietarios de los sistemas de información.

4.4 ISACA.

A lo largo de este apartado daremos una visión general de ISACA, en la que describiremos cuáles son sus funciones, quiénes son sus miembros y qué repercusiones tienen sus decisiones en las organizaciones dedicas a los sistemas de información.

Comenzó en el año 1.967 cuando un pequeño grupo de personas que realizaban trabajos similares sobre los sistemas computarizados llegaron a la conclusión de que era necesario crear un organismo que centralizara y además sirviera de guía para dichos trabajos.

Durante el año 1.969 esta idea tomo cuerpo y se formo el EDP Auditors Association. En 1.976 formaron una fundación de educación para investigar a gran escala y expandir los conocimientos en los campos de gobernación y de Investigación y Tecnología.

En la actualidad los miembros del comité se encuentran en la totalidad de los países desarrollados, y en su mayoría trabajan en el sector de Investigación y Tecnología desempeñando funciones de auditor, consultor, educador, profesional de seguridad, regulador… Aunque también trabajan en industrias, finanzas, banca, en el sector público, contabilidad, manufactura…

Esta gran diversidad ha permitido que los miembros aprendan unos de otros, consiguiendo puntos de vista de todo tipo y de todos los sectores.

Sus normas y estándares de auditoría y de sistemas de información son respetadas por los profesionales de todo el mundo ya que son un símbolo de calidad.

A continuación detallamos los más importantes:

Estatuto de auditoría

Propósito, responsabilidad, autoridad y rendición de cuentas de la función de auditoría de sistemas de información o de las asignaciones de auditoría de sistemas de información deben documentarse de manera apropiada en un estatuto de auditoría o carta de compromiso.

El estatuto de auditoría o la carta de compromiso deben ser aceptados y aprobados en el nivel apropiado dentro de la organización.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Enero de 2.005.

Independencia de Auditoría de Sistemas de Información.

Independencia profesional en todos los aspectos relacionados con la auditoría, el auditor de sistemas de información debe ser independiente del auditado, tanto en actitud como en apariencia.

Independencia organizacional, la función de auditoría de sistemas de información debe ser independiente del área o actividad que se está revisando para permitir una conclusión objetiva de la tarea que se audita.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Enero de 2.005.

Ética y Normas Profesionales de Auditoría de S.I.

El auditor de Sistemas de Información debe cumplir con el Código de Ética Profesional de ISACA al realizar tareas de auditoría.

El auditor de Sistemas de Información debe ejercer el debido cuidado profesional, lo cual incluye cumplir con los estándares profesionales de auditoría aplicables al realizar tareas de auditoría.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Enero de 2.005.

Competencia Profesional de Auditoría de S.I.

El auditor de Sistemas de Información debe ser profesionalmente competente y tener las destrezas y los conocimientos para realizar la tarea de auditoría.

El auditor de sistemas de información debe mantener competencia profesional por medio de una apropiada educación y capacitación profesional continua.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Enero de 2.005.

Planificación de Auditoría de Sistemas de Información.

El auditor de sistemas de información debe planear la cobertura de la auditoría de sistemas de información para cubrir los objetivos de la auditoría y cumplir con las leyes aplicables y las normas profesionales de auditoría.

El auditor de sistemas de información debe desarrollar y documentar un enfoque de auditoría basado en riesgos.

El auditor de sistemas de información debe desarrollar y documentar un plan de auditoría que detalle la naturaleza y los objetivos de la auditoría, los plazos y alcance, así como los recursos requeridos.

El auditor de sistemas de información debe desarrollar un programa y/o plan de auditoría detallando la naturaleza, los plazos y el alcance de los procedimientos requeridos para completar la auditoría.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Enero de 2.005.

Realización de Labores de Auditoría de S.I.

El personal de auditoría de sistemas de información debe ser supervisado para brindar una garantía razonable de que se lograrán los objetivos de la auditoría y que se cumplirán las normas profesionales de auditoría aplicables.

Durante el transcurso de la auditoría, el auditor de sistemas de información debe obtener evidencias suficientes, confiables y pertinentes para alcanzar los objetivos de auditoría. Los hallazgos y conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia.

El proceso de auditoría deberá documentarse, describiendo las labores de auditoría realizadas y la evidencia de auditoría que respalda los hallazgos y conclusiones del auditor de sistemas de información.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Enero de 2.005.

Reporte de Auditoría de Sistemas de Información

El auditor de sistemas de información debe suministrar un informe, en un formato apropiado, al finalizar la auditoría. El informe debe identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación.

El informe de auditoría debe indicar el alcance, los objetivos, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.

El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el auditor de sistemas de información tuviese en cuanto al alcance de la auditoría.

El auditor de sistemas de información debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.

Al emitirse, el informe del auditor de sistemas de información debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta de compromiso.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Enero de 2.005.

Actividades de Seguimiento de Auditoría de S.I.

Después de informar/reportar sobre hallazgos y las recomendaciones, el auditor de sistemas de información debe solicitar y evaluar la información relevante para concluir si la gerencia tomó las acciones apropiadas de manera oportuna.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Enero de 2.005.

Irregularidades y Acciones Ilegales de Auditoría de S.I.

Al planificar y realizar la auditoría para reducir el riesgo de auditoría a un nivel bajo, el auditor de sistemas de información debe tener en cuenta el riesgo de irregularidades y acciones ilegales.

El auditor de sistemas de información debe mantener una actitud de escepticismo profesional durante la auditoría, reconociendo la posibilidad de que podrían existir declaraciones materialmente incorrectas debido a irregularidades y acciones ilegales, independientemente de su propia evaluación del riesgo de irregularidades y acciones ilegales.

El auditor de sistemas de información debe obtener un entendimiento de la organización y su entorno, incluidos los controles internos.

El auditor de sistemas de información debe obtener evidencia de auditoría suficiente y relevante para determinar si la gerencia u otras personas dentro de la organización tienen conocimientos de cualquier irregularidad y acción ilegal real, sospechada o alegada.

Al realizar procedimientos de auditoría para obtener un entendimiento de la organización y su entorno, el auditor de sistemas de información debe considerar relaciones inusuales o inesperadas que pueden indicar un riesgo de declaraciones materialmente incorrectas debido a irregularidades y acciones ilegales.

El auditor de sistemas de información debe diseñar y realizar procedimientos para probar lo adecuado de los controles internos y el riesgo de anulación de los controles por parte de la gerencia.

Cuando el auditor de sistemas de información identifica una declaración incorrecta, el auditor de sistemas de información debe evaluar si tal declaración incorrecta puede indicar la existencia de una irregularidad o acción ilegal. Si existe tal indicación, el auditor de sistemas de información debe tener en cuenta las implicaciones en relación con otros aspectos de la auditoría y, en particular, las declaraciones de la gerencia.

El auditor de sistemas de información debe obtener declaraciones escritas de la gerencia al menos una vez al año con mayor frecuencia, dependiendo del contrato de auditoría. La gerencia debe:

- Reconocer su responsabilidad en el diseño e implementación de controles internos para prevenir y detectar irregularidades o acciones ilegales.

- Revelar al auditor de sistemas de información los resultados de la evaluación de riesgos cuando pueda existir una declaración materialmente incorrecta como resultado de una irregularidad o acción ilegal.
- Revelar al auditor de sistemas de información cuando tenga conocimiento de irregularidades o acciones ilegales que estén afectando a la organización en relación a la gerencia y empleados que tienen funciones significativas en el control interno.
- Revelar al auditor de sistemas de información cuando tenga conocimientos de cualquier declaración de irregularidades o acciones ilegales, o sospechosas de irregularidades o acciones ilegales que estén afectando la organización tal como lo hayan comunicado los empleados, ex empleados, funcionarios responsables de la normatividad dentro de la organización.

Si el auditor de sistemas de información ha identificado una irregularidad material o acción ilegal, u obtiene información de que puede existir una irregularidad material o acción ilegal, el auditor de sistemas de Información debe comunicarlo sin demora al nivel de dirección apropiado.

Si el auditor de sistemas de información ha identificado una irregularidad material o acción ilegal que involucra a la gerencia o a empleados que tienen funciones significativas en el control interno, el auditor de sistemas de información debe comunicarlo sin demora a los responsables del gobierno corporativo.

El auditor de sistemas de información debe dar recomendaciones al nivel apropiado de la gerencia y a aquellos responsables del gobierno corporativo

sobre las debilidades materiales en el diseño e implementación del control interno para prevenir y detectar irregularidades y acciones ilegales que el auditor de sistemas de información pueda haber notado durante la auditoría.

Si el auditor de sistemas de información encuentra circunstancias excepcionales que afectan su capacidad para continuar ejecutando la auditoría debido a una declaración materialmente incorrecta o una acción ilegal, el auditor de sistemas de información debe tener en cuenta la responsabilidad legal y profesional aplicable en tales circunstancias, incluyendo que pueda existir el requisito para el auditor de sistemas de información de notificar a aquellos que celebraron el contrato o, en algunos casos, a los responsables del gobierno corporativo o a las autoridades responsables de la normatividad dentro de la organización o incluso considerar retirarse del contrato.

El auditor de sistemas de información debe documentar todas las comunicaciones, planificación, resultados, evaluaciones y conclusiones relacionadas con irregularidades materiales y acciones ilegales que han sido notificadas a la gerencia, a los responsables del gobierno corporativo, autoridades responsables de la normatividad dentro de la organización.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Septiembre de 2.005.

Gobernabilidad de Tecnologías de Información en Auditoría de Sistemas de Información.

El auditor de sistemas de información debe revisar y evaluar si la función de sistemas de información está alineada con la misión, visión, valores, objetivos y estrategias de la organización.

El auditor de sistemas de información debe revisar si la función de sistemas de información tiene una declaración clara en cuanto al desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.

El auditor de sistemas de información debe revisar y evaluar la eficacia de los recursos de sistemas de información y el desempeño de los procesos administrativos.

El auditor de sistemas de información debe revisar y evaluar el cumplimiento de los requisitos legales, ambientales y de calidad de la información, así como de los requisitos fiduciarios y de seguridad.

El auditor de sistemas de información debe utilizar un enfoque basado en riesgos para evaluar la función de sistemas de información.

El auditor de sistemas de información debe revisar y evaluar el ambiente de control de la organización.

El auditor de sistemas de información debe revisar y evaluar los riesgos que pueden afectar de manera adversa el entorno de sistemas de información.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Septiembre de 2.005.

Uso de la Evaluación de Riesgos en la Planificación de Auditoría de Sistemas de Información.

El auditor de sistemas de información debe utilizar una técnica o enfoque apropiado de evaluación de riesgos al desarrollar el plan general de auditoría de sistemas de información y al determinar prioridades para la asignación eficaz de los recursos de auditoría de sistemas de información.

Al planear revisiones individuales, el auditor de sistemas de información debe identificar y evaluar los riesgos relevantes al área bajo revisión.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Noviembre de 2.005.

Materialidad de Auditoría de Sistemas de Información.

El auditor de sistemas de información debe considerar la materialidad de la auditoría y su relación con el riesgo de auditoría a la vez que determina la naturaleza, los plazos y el alcance de los procedimientos de auditoría.

Mientras planifica la auditoría, el auditor de sistemas de información debe considerar las posibles debilidades o la ausencia de controles, y si tales debilidades o ausencias de controles pueden ocasionar una deficiencia importante o una debilidad material en el sistema de información.

El auditor de sistemas de información debe considerar el efecto acumulativo de las deficiencias o debilidades menores de control y la ausencia de controles que pueden traducirse en una deficiencia significativa o debilidad material en el sistema de información.

El informe del auditor de sistemas de información debe divulgar los controles ineficaces o la ausencia de controles, y el significado de estas deficiencias, así como la posibilidad de que estas debilidades ocasionen una deficiencia importante o debilidad material.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Julio de 2.006.

Uso del Trabajo de Otros Expertos en Auditoría de S.I.

El auditor de sistemas de información debe, donde resulte apropiado, considerar el uso del trabajo de otros expertos para realizar la auditoría.

El auditor de sistemas de información debe evaluar y estar satisfecho con las credenciales profesionales, competencias, experiencia relevante, recursos,

independencia y procesos de control de calidad de otros expertos, antes de su contratación.

El auditor de sistemas de información debe evaluar, revisar y calificar el trabajo de otros expertos como parte de la auditoría y concluir el grado de utilidad y la fiabilidad del trabajo experto.

El auditor de sistemas de información debe determinar y concluir si el trabajo de otros expertos resulta adecuado y suficiente para permitir que el auditor de sistemas de información saque sus conclusiones con respecto a los objetivos actuales de la auditoría. Dicha conclusión debe documentarse claramente.

El auditor de sistemas de información debe aplicar procedimientos de prueba adicionales para lograr una evidencia de auditoría suficiente y apropiada en circunstancias en las que el trabajo de otros expertos no la proporciona.

El auditor de sistemas de información debe proporcionar una opinión de auditoría apropiada e incluir los límites del alcance cuando no se obtenga la evidencia requerida mediante procedimientos de prueba adicionales.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Julio de 2.006.

Evidencia de Auditoría de Sistemas de Información.

El auditor de sistemas de información debe obtener evidencias de auditoría suficientes y apropiadas para llegar a conclusiones razonables sobre las que basar los resultados de la auditoría.

El auditor de sistemas de información debe evaluar la suficiencia de las evidencias de auditoría obtenidas durante la misma.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Julio de 2.006.

Controles de Informática y Tecnología en Auditoría de S.I.

El auditor de sistemas de información debe evaluar y supervisar los controles de informática y tecnología que son parte integral del entorno de control interno de la organización.

El auditor de sistemas de información debe asistir a la gerencia proporcionando consejos con respecto al diseño, la implementación, la operación y la mejora de controles de informática y tecnología.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Febrero de 2.008.

Comercio Electrónico en Auditoría en S.I.

El auditor de sistemas de información debe evaluar los controles aplicables, y cotejar los riesgos al revisar entornos de comercio electrónico, para asegurar que las transacciones de comercio electrónico están correctamente controladas.

Este estándar para la auditoría de sistemas de información está vigente desde el 1 de Febrero de 2.008.

Servicios de internet.

Dentro de los estándares de ISACA, este no es de los más importantes, pero debido a la naturaleza del presente proyecto final de carrera hemos creído interesante su inclusión.

En la actualidad internet ofrece una gran diversidad de servicios, y prácticamente a diario aparecen servicios nuevos, y no únicamente para ordenadores, sino también para móviles, agendas electrónicas, videoconsolas,…

Aunque uno de los servicios más importantes que se ofrecen actualmente en internet es el correo electrónico, parte de su importancia radica en que es el servicio más utilizado.

En la actualidad el correo electrónico es más utilizado que el correo postal tradicional. Aunque no fue diseñado para ser un servicio seguro, sino como un medio alternativo al fax y al correo postal mucho más barato, por lo que en la práctica es un servicio con un alto déficit de seguridad. Los puntos más débiles del correo electrónico son los siguientes:

- **Imposibilidad de autentificar al remitente.** Es imposible conocer realmente si el remitente que aparece en el correo electrónico es el remitente real o si ha sido suplantado.

  Aunque esta debilidad puede ser subsanada mediante la utilización de firmas electrónicas, lo que es muy común en relaciones comerciales y profesionales, aunque es muy poco usual en comunicaciones entre particulares.
- **Los mensajes enviados a través internet no tienen formato.**

  Debido a esta debilidad es bastante posible que cualquier persona pueda tener acceso al mensaje para leerlo o incluso para modificarlo. Esta debilidad puede solucionarse cifrando el contenido del mensaje.
- **No se puede garantizar que la entrega del mensaje se haya realizado de forma segura.** Lo normal es que un mensaje se entrega en unos pocos segundos o minutos, aunque en algunos casos la entrega se puede retrasar durante horas por problemas en los distintos servidores de correo, tanto del remitente como del destinatario.

Dependiendo de la configuración de los servidores de correo, el remitente del mensaje puede recibir la notificación de que su mensaje no ha sido entregado, de forma casi inmediata, o pueden llegar a pasar días o incluso puede que no reciba ninguna notificación al respecto.

- **Ficheros adjuntos al correo electrónico.** Muchas organizaciones utilizan el servicio de correo electrónico para enviar documentos adjuntos al texto del propio correo electrónico.

  Debido a que en bastantes ocasiones los datos adjuntos son muy grandes, algunas organizaciones han puesto restricciones en cuanto al tamaño de los ficheros adjuntos al correo electrónico, para evitar sobrecargas en los servidores, tanto de procesamiento como de capacidad de las cuentas de correo.

- **Recepción de SPAM.** El SPAM son todos aquellos correos no deseados que se reciben en los que se intenta vendernos algún producto de dudosa procedencia y/o utilidad.

  Aunque es considerado un problema de seguridad sencillo puede llegar a ser un verdadero quebradero de cabeza para los administradores de correo electrónico, pues un envío masivo de SPAM puede llegar a colapsar los servicios de correo electrónico.

4.5 ISO 27002.

A lo largo de este punto hablaremos sobre el estándar ISO 27002, promulgado por la Organización Internacional de Estandarización, hemos creído conveniente incluir este punto en el actual proyecto fin de carrera, porque en dicho estándar se asientan las bases de la seguridad de la información.

Es un estándar internacional que establece los principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

Los objetivos de control y los controles de este estándar han sido diseñados para ser implementados de forma que satisfagan los requerimientos identificados por una evaluación del riesgo.

Dentro de este estándar se definen la evaluación y el tratamiento del riesgo, las diferentes políticas de seguridad, las distintas organizaciones de la seguridad de la información, la gestión de archivos, la seguridad de los recursos humanos, la seguridad física y ambiental, la gestión de las comunicaciones y las operaciones, el control de acceso, la adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de los posibles incidentes en la seguridad de la información, gestión de la continuidad del negocio y por último el cumplimiento de las distintas leyes.

No hemos creído necesario entrar en detalle en ninguno de los distintos puntos de este estándar, ya que aquellos puntos del estándar que son importantes para el desarrollo del presente proyecto final de carrera, han sido utilizados como una de las principales referencias para desarrollar dichos puntos de la memoria del proyecto final de carrera. Aunque en el anexo b del

presente proyecto final de carrera sí que se definen los diferentes puntos del estándar.

4.6 CONCLUSIONES RESPECTO A LA NORMATIVA LEGAL VIGENTE.

Tras la lectura detenida de la distinta normativa que rige los sistemas de información y en particular el correo electrónico hemos llegado a las siguientes conclusiones:

Todo procesamiento llevado a cabo por los sistemas de información siempre debe de tener al menos una persona responsable del mismo, que asegure en todo momento que se cumple tanto la normativa legal vigente como la normativa interna de la propia organización.

Cualquier tipo de transferencia o de modificación sobre ficheros que contengan datos de carácter personal deberá ser autorizada por el responsable del fichero, y dicha autorización se deberá atener a la legalidad, por lo que sólo se podrá realizar en aquellos casos en los que la ley lo autorice de forma expresa.

Cualquier tipo de transacción realizada de forma electrónica conlleva los mismos derechos y obligaciones que una transacción tradicional para todas las partes implicadas en la misma.

Todo servicio prestado de forma electrónica ha de tener un responsable legal, ya sea físicamente una persona o una organización, para poder asegurar de esta forma que se cumple la legalidad y que se conservan los derechos y obligaciones tanto de los usuarios como de la organización prestadora del servicio.

Toda organización debe desarrollar los mecanismos necesarios para asegurar que se cumple la ley en todo momento. Entre estos mecanismos se

deberán incluir los necesarios para asegurar la seguridad de la información y de las comunicaciones, tanto a nivel interno como externo. Con relación a esto hay una gran controversia, ya que las organizaciones utilizan la necesidad de cumplir la normativa legal como argumento para poder controlar todas las comunicaciones y procesamiento de datos que se producen en todos sus sistemas, incluidos los ordenadores de sus empleados. En ningún punto de la normativa legal vigente se autoriza de forma explícita esta conducta como medida de seguridad, es más, este tipo de conductas pueden llegar a constituir un delito, puesto que espiar tanto los correos electrónicos o documentos personales de los empleados puede vulnerar el derecho a la intimidad de los mismos. Actualmente no hay ningún sistema que permita discriminar a priori que información o comunicación electrónica es privada y cual es profesional, debido a esto ninguna organización debería tratar de controlar todas sus comunicaciones y documentos, sino que deberían limitar el acceso de sus empleados a ciertos tipos de programas y de comunicaciones. También es importante destacar, que hay ciertos casos en los que se entiende e incluso se considera legal, el acceso por parte de la organización al correo electrónico de un empleado o incluso a su ordenador, estos casos son aquellos en los que por diversos motivos no es posible contactar con el empleado (está de vacaciones, ha sufrido un accidente, está en una zona sin cobertura,…) y es de vital importancia para la organización tener acceso a esos datos, ya sea porque en el ordenador del empleado están todos los datos de los clientes, los pedidos recibidos, los datos del IRPF del resto de empleados,…

5. AUDITORÍA INFORMÁTICA.

5.1 INTRODUCCIÓN.

Hemos creído de vital importancia la inclusión de este punto en el actual proyecto final de carrera, ya que al tratarse de un proyecto cuyo tema principal es la auditoría informática, es fundamental explicar de forma genérica en qué consiste una auditoría antes de comenzar a realizar la propia auditoría. De esta forma intentamos conseguir que cualquier persona que pueda leer el presente proyecto final de carrera, tenga una idea genérica de qué es una auditoría informática, ya que no esperamos que el proyecto sea un manual de referencia para expertos en auditoría informática, sino que sirva de ayuda a cualquier persona no iniciada ni en el mundo de la auditoría informática ni en Lotus Notes, ya que consideramos que un experto en alguno de estos dos temas o en ambos, posee unos conocimientos muy superiores a los mostrados a lo largo del presente proyecto final de carrera.

Actualmente la información alojada en los sistemas de información es de vital importancia para la supervivencia de las organizaciones, ya que es un activo más de la organización y gracias al mismo la organización puede sobrevivir y competir con el resto de organizaciones de su sector.

Por lo tanto, las organizaciones deberán implementar los sistemas necesarios para asegurar la información, ya sea de desastres naturales o provocados, de delitos o errores humanos y optimizar los recursos, racionalizar costes e incrementar la calidad de sus productos.

También se debe tener en cuenta que para mantener la posición en el mercado de la organización o incluso mejorarla, los entornos de producción de las organizaciones son cada vez más complejos, esto es causado en gran medida por las nuevas tecnologías de comunicación, de dispositivos móviles o incluso sistemas de inteligencia artificial.

Por estas razones, las organizaciones han debido diseñar ciertas líneas de contención que aseguren sus sistemas frente a ataques externos e incluso internos, algunas de estas líneas de contención pueden ser la creación de diversos controles (en los sistemas, para los empleados, para las instalaciones,…), inspecciones sorpresa del funcionamiento de los sistemas y del comportamiento de los empleados, auditorías (tanto internas como externas), separar las funciones y las responsabilidades de los distintos empleados en función de los puestos que ocupen, y crear responsables de áreas de seguridad, auditoría,…

5.2 CONTROL INTERNO.

Todas las organizaciones han de tener una serie de controles internos que les permitan conocer el estado de sus sistemas y que con la implantación de los mismos puedan evitar accesos no autorizados, errores en los sistemas o posibles vulnerabilidades.

Podemos definir control interno como toda actividad o acción realizada por uno o varios elementos (humanos, máquinas,…) que prevenga, detecte o corrija algún error, omisión o irregularidad que afecte al funcionamiento de alguna parte de la organización. Cuanto mejores y mayores sean los controles menos probabilidades de errores habrá, aunque cabe destacar que no tiene sentido invertir más recursos en diseñar nuevos controles que el valor estimado del recurso a proteger. La creación de los controles es responsabilidad únicamente de la dirección de la organización, aunque los controles son realizados por los supervisores y son verificados por los auditores.

Las principales características de los controles son:

- **Simple:** Para controlar un posible error no es necesario que el proceso sea complicado de entender, y que su funcionamiento y su estructura sean enrevesadas.
- **Completo:** Debe contemplar todos los escenarios posibles, sin dejar de comprobar ninguna opción que se pueda producir durante el funcionamiento normal o atípico de los sistemas.
- **Operativo:** Debe de ser rápido en su comprobación, para detectar de forma rápida el problema y evitar que dicho problema se replique en otras partes de los sistemas de información de la organización.

- **Fiable:** No debe de producir fallos durante sus comprobaciones y debe de estar siempre en funcionamiento.
- **Revisable:** Una vez que ha sido implantado debe de ser posible realizar futuras mejoras sobre el mismo.
- **Práctico:** Debe solucionar, detectar o prevenir algún error, omisión o irregularidad.
- **Razonable:** Su coste debe de ser bajo en recursos humanos, técnicos y económicos.
- **Adecuado:** No debe de realizar comprobaciones ya realizadas en controles precedentes o posteriores, ya que de ser así habría algún control mal diseñado y que por lo tanto sería prescindible.
- **Rentable:** El coste de implantar el control en ningún caso debe de ser más elevado que el valor del bien a proteger.

A continuación enumeramos los principales tipos de control:

- **Tipo de control directivo**. Se centran en crear políticas, procedimientos y secuencias de tareas. Algún ejemplo de este tipo de control puede ser la creación de una auditoría interna o la creación de un grupo de seguridad dentro de la organización.
- **Tipo de control preventivo**. Se centran en el momento anterior al error, omisión o irregularidad, es decir, con su creación se intenta evitar que se produzca cualquier tipo de fallo. Algún ejemplo de este tipo de control puede ser los paquetes o dispositivos de acceso o las duplas usuario-contraseña.

- **Tipo de control de detección.** Se centran en intentar averiguar si se ha producido cualquier tipo de error, básicamente se consigue realizando seguimientos sobre los controles preventivos y revisando si se produce alguna operación contra la normativa de la organización. Algún ejemplo de este tipo de control puede ser la revisión de los ficheros de log.
- **Tipo de control correctivo.** Se centran en una vez detectado el problema en tratar de solucionar el mismo. Algún ejemplo de este tipo de control puede ser la recuperación de un fichero dañado total o parcialmente.
- **Tipo de control de recuperación.** Se centran en recuperar el sistema a un estado anterior en el que su funcionamiento era correcto. Algún ejemplo de este tipo de control puede ser tener equipos duplicados en diferentes zonas.

5.3 ¿QUÉ ES LA AUDITORÍA INFORMÁTICA?

Podemos definir la auditoría informática como el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

En la actualidad no existe ningún tipo de legislación que indique qué personas y bajo qué condiciones pueden realizar una auditoría informática, aunque como hemos mencionado en el punto 4 del presente proyecto final de carrera, la normativa vigente si exige una serie de mínimos de seguridad que deben cumplir las organizaciones, pero no indica quiénes deben ser los encargados de realizarlos ni qué titulación mínima han de poseer.

Aunque muchas personas piensen que auditoría es lo mismo que consultoría en realidad no es así, aunque es cierto que tienen muchos puntos en común y que en ocasiones las personas encargadas de realizar una u otra se basan en la información y material aportados por la otra. Además las personas que las realizan tienen bastantes puntos en común como pueden ser una formación y una experiencia muy similar, han de ser personas con independencia, objetividad, una gran ética profesional, penetración psicológica y madurez, no deben revelar informaciones confidenciales de la organización y tienen competencias en áreas similares. Por el contrario también tienen puntos que las diferencian ampliamente como el objetivo, en la auditoría el objetivo principal es redactar un informe que contemple las medidas que deberían tomarse en la organización, teniendo en cuenta la normativa legal y la propia de la organización, que indique además cuales se cumplen y que recomiende que

medidas deberían tomarse para cumplir la normativa o cumplirla de forma más eficiente; por el contrario el objetivo de la consultoría es asesorar a las organizaciones en relación a los distintos productos existentes que solucionan una o varias necesidades conocidas de la organización, este tipo de necesidades suelen estar relacionadas con la implantación de algún nuevo sistema de información o con la actualización o modificación de alguno ya existente en la organización, lo que también conlleva realizar un informe; pero este será muy distinto al generado por la auditoría, ya que como hemos comentado sus objetivos son diferentes.

Tipos de auditoría.

Podemos definir varios tipos de auditoría en función del objetivo de la misma, aunque una misma auditoría puede ser tener varios tipos a la vez:

- **De control:** El principal objetivo de este tipo de auditoría es comprobar que todos los sistemas de control y verificación de la organización se cumplen correctamente y evaluar si existe la posibilidad de añadir nuevos controles o modificar los controles ya existentes para evitar necesidades futuras de la organización a corto plazo.

  En el caso que uno o varios controles no funcionen correctamente o puedan ser modificados para obtener un mejor rendimiento, se indicará en el informe final de auditoría.
- **De cumplimiento:** El principal objetivo de este tipo de auditoría es comprobar que la organización cumple toda la normativa que

considera aplicable, tanto interna de la propia organización como a nivel estatal o internacional.

Todos aquellos puntos de la normativa que no se cumplan aparecerán reflejados en el informe final de auditoría.

- **De seguridad:** El principal objetivo de este tipo de auditoría es comprobar si todos los sistemas de información de la organización y todas sus comunicaciones se realizan de forma segura y mediante los sistemas de seguridad necesarios, por lo que es poco probable que puedan verse afectados.

  Si se hallarán deficiencias en los sistemas de seguridad se debería indicar en el informe final de auditoría.

- **De gestión:** El principal objetivo de este tipo de auditoría es comprobar la eficiencia y la eficacia de la organización a todos sus niveles, desde la alta dirección hasta el departamento más pequeño e insignificante de la organización.

  En el caso que uno o varios departamentos o servicios de la organización no sean eficientes o eficaces se indicarán las probables causas de dichas deficiencias en el informe final de auditoría.

- **De apoyo a la auditoría de cuentas:** El principal objetivo de este tipo de auditoría es servir como ayuda y referencia de la auditoría de cuentas, que es completamente independiente a la auditoría informática, pero que sin la ayuda de la auditoría informática actualmente no sería posible realizar ninguna auditoría de cuentas, ya que casi la totalidad de las organizaciones tienen informatizados casi todos sus procesos.

- **De investigación de delitos o fraudes:** El principal objetivo de este tipo de auditoría es averiguar si dentro de una organización se ha producido algún tipo de delito o fraude, ya haya sido de forma intencionada o por descuido.

  Para ello se trata de verificar que todos los accesos a los sistemas y modificaciones de los datos se han realizado en la forma y manera que se especifica en la normativa de la organización, de no ser así se trata de comprobar de qué forma se produjo el acceso o la modificación de los datos y todas estas anomalías deben quedar reflejadas en el informe final de auditoría.

- **De relaciones con los recursos humanos:** El principal objetivo de este tipo de auditoría es comprobar que las comunicaciones que realiza el departamento de recursos humanos con los sistemas de información de la organización se realizan en la forma indicada en la normativa.

  Si en algún punto no se cumple la normativa debe quedar reflejado en el informe final de auditoría.

- **De reglamento legal:** El principal objetivo de este tipo de auditoría es comprobar que la organización contempla toda la normativa legal que es aplicable a la organización en función de sus actividades, esta normativa es tanto a nivel estatal como internacional.

  En el caso que se encontrase alguna norma, directiva o ley que no fuese contemplada por la organización o que se implementase de forma deficiente debería quedar reflejado en el informe final de auditoría.

También podemos definir varios tipos de auditoría en función de si las personas que la realizan son empleados de la organización o no.

- **Interna:** Este tipo de auditoría es realizada por el propio personal de la organización. Por este motivo tiene un gran nivel de acceso al personal, a los datos de los sistemas, a los documentos, contratos, actas,…En principio el acceso al material sólo será limitado por la alta dirección y en función del objetivo de la auditoría.

  A priori este tipo de auditoría no será ni tan independiente ni tan objetivo como la auditoría externa, ya que parece obvio que las personas que realizarán la auditoría estarán sujetas a mayores presiones por parte de la directiva y de los jefes de sección, y también por el resto de compañeros e incluso por sus jefes.

  En función del objetivo de la auditoría el destinatario del informe de la misma puede ser un jefe de sección en concreto, un departamento o incluso algún miembro de la dirección, aunque también el destinatario del informe puede ser su jefe directo.

  Para que una auditoría interna tenga el mayor grado de independencia y objetividad posible, sólo debe depender jerárquicamente o de la alta dirección de la organización o del auditor general, ya que si depende jerárquicamente del director de algún departamento o área de la organización los miembros de la auditoría estarán sujetos a un mayor número de presiones por parte de su jefe directo para que su sección o área aparezca en la auditoría de la mejor forma posible. Debido a esto es conveniente que exista un comité de auditoría independiente que pueda mediar en los

posibles conflictos derivados de la elaboración del informe de auditoría.

A la hora de crear una auditoría interna habrá que tener en cuenta diversos factores, en primer lugar habrá que tener en cuenta la profundidad y objetivo de la misma, que personas dentro de la organización van a tomar parte en la misma y que ventajas (formación, experiencia,…) y desventajas (funciones que desempeñan actualmente, antiguos compañeros,…) aportarían a la realización del informe final de auditoría.

- **Externa:** Este tipo de auditoría es realizada por personal ajeno a la organización contratado exclusivamente para llevar a cabo el informe de auditoría.

  La auditoría de cuentas siempre se acompaña de una auditoría informática, como hemos comentado anteriormente, aunque no habíamos mencionado que se trata de una auditoría informática externa. Tanto el objetivo de la auditoría como el destinatario del informe de la misma es designado por la persona, departamento o ente que encargó la realización de la misma, normalmente este tipo de auditorías suelen ser encargadas por la alta dirección, un grupo mayoritario de accionistas,…

Las auditorías internas y externas no son excluyentes, sino que por el contrario se complementan, es más, para que una organización se pueda considerar perfectamente auditada debería tener un departamento dedicado única y exclusivamente a la realización de auditorías internas del resto de departamentos y periódicamente se deberían realizar auditorías externas.

En el caso que existan auditorías internas, las auditorías externas pueden usar el trabajo de los internos de forma complementaria al suyo propio para obtener una mayor profundidad y calidad del informe de auditoría final, además los externos pueden aportar nuevas técnicas y métodos que sirvan en el futuro a los internos e incluso puede darse el caso que la auditoría interna sea creada posteriormente a la externa, porque se incluya en su informe de auditoría la creación de una auditoría interna como recomendación.

A la hora de realizar una auditoría informática, sea del tipo que sea, hay que tener claro cuál es el objetivo de la auditoría, a qué ámbito de la organización se evaluará y las restricciones a las que estará sujeta la auditoría.

En primer lugar, antes de comenzar una auditoría se debe realizar un trabajo previo en el que se realiza un presupuesto, una planificación general y por último el programa de trabajo, todo ello se muestra a la persona interesada en contratar los servicios de auditoría para su aprobación.

En segundo lugar se realiza el trabajo de campo que consiste en realizar trabajos, entrevistas, pruebas,… para evaluar el estado de la organización y obtener los datos suficientes para poder realizar el informe final de auditoría.

Por último realizaremos el informe de auditoría, en primer lugar se crea un borrador que será revisado con el resto del grupo de trabajo y con las notas tomadas por el equipo para su discusión y de esta forma tratar de llegar a un consenso para presentar el informe de auditoría definitivo al cliente. Posteriormente hablaremos más en detalle de la elaboración del informe de auditoría, aunque ahora comentaremos las fuentes necesarias para la realización del informe:

- Políticas, estándares y procedimientos de la organización.
- Planes informáticos.
- Organigramas y comités.
- Presupuestos y seguimientos.
- Informes de auditorías anteriores.
- Nuestra propia documentación generada durante el trabajo de campo.
- Actas de reuniones relacionadas con la auditoría.
- Informes de proveedores, consultores,…
- Memorandos, circulares, comunicados,…
- Memorias de la organización.
- Intranet de la organización.
- Planos de los edificios, accesos, acometidas de suministros,…
- Software alojado en los sistemas de información de la empresa.
- Redes de comunicaciones.
- Pólizas de seguros contratadas.
- Contratos con prestadores de servicios.

5.4 LA FIGURA DEL AUDITOR INFORMÁTICO.

Hemos creído necesario hablar de la figura del auditor informático para que de esta forma quede un poco más claro cómo debe realizarse una auditoría informática, ya que a lo largo de este punto enumeraremos las principales características que debe tener un buen auditor informático, y por lo tanto estas cualidades deberían aflorar durante la elaboración de la auditoría.

Podemos definir auditor informático como toda persona profesional de los sistemas de información encargada de realizar informes de auditoría informática.

Para que un auditor pueda desempeñar correctamente sus funciones debe mantener unas cordiales relaciones con todo el organigrama de la organización que auditará, es decir, no debe mantener ningún tipo de conflicto con la dirección, los distintos departamentos o áreas, con el resto de miembros de la auditoría externa y si procede con los miembros de la interna, con los consultores y asesores,…

Un buen auditor ha de tener las siguientes cualidades:

- **Formación:** Ha de tener una serie de conocimientos en sistemas de información y en auditoría mínimos que le permitan realizar sus funciones con total garantía de éxito.
- **Experiencia:** Ha de tener la suficiente experiencia tanto en sistemas de información, en la realización de informes y por supuesto en auditoría.

- **Independencia y objetividad:** Estas dos cualidades son indispensables para poder realizar un informe de auditoría con la suficiente calidad y rigor, ya que si alguna de las dos no se cumple el informe quedará viciado.
- **Madurez:** Ha de tener la suficiente madurez como para poder analizar situaciones complejas y para realizar un informe de auditoría de forma profesional.
- **Integridad y ética:** Estas dos cualidades son indispensables para todo auditor ya que sin ellas, el informe redactado no tendría ningún valor, ya que no reflejaría la situación real.
- **Capacidad de análisis y síntesis:** Estas dos cualidades son necesarias para que cualquier auditor pueda observar las deficiencias de la organización y plasmarlas en el informe de auditoría con el suficiente grado de resumen, para que el informe no sea demasiado extenso y tedioso.
- **Seguridad en sí mismo:** Sin esta cualidad el auditor podría dudar demasiado en sus afirmaciones y ser fácilmente cuestionado, quitándole de esta forma importancia o gravedad a las mismas.
- **Responsabilidad:** Ha de tener esta cualidad para que la persona que encargo el informe de auditoría confíe en él para darle acceso al material y los sistemas de información de la organización necesarios para realizar el informe.
- **Interés:** Sin esta cualidad el auditor realizaría un informe de auditoría muy pobre y escaso, ya que sin interés no profundizaría en

los posibles problemas o defectos de la organización y de sus sistemas de información.

Para todo auditor informático es de vital importancia el continuo aprendizaje ya sea a través de cursos, seminarios o incluso de trabajos, puesto que en la actualidad los sistemas de información se están mejorando continuamente y modificando sus tecnologías, por lo tanto los conocimientos usados durante un año, puede que al año siguiente se hayan quedado obsoletos.

Hay que tener presente que un buen auditor informático lo ha de ser siempre, es decir, que si durante el desempeño de una auditoría informática o cualquier otro tipo de trabajo que se esté desempeñando detecta alguna deficiencia, vulnerabilidad, defecto,… en la organización o en sus sistemas de información debería comunicárselo a los responsables del mismo ya fuera por escrito o verbalmente siempre que el trabajo que estuviese desempeñando en el momento de la localización del defecto no fuese una auditoría informática de ese sistema de información, ya que en ese caso la deficiencia quedaría reflejada en el informe final de auditoría.

Hay que tener presente que aunque hemos estado hablando de la figura del auditor informático, éste no trabaja sólo, sino que forma parte de un grupo de trabajo, dentro del cual puede desempeñar algún otro rol a parte del auditor.

El grupo de trabajo para realizar una auditoría suele estar formado por al menos un gerente, un jefe de equipo y un auditor, aunque una misma persona puede desempeñar diferentes roles, en ocasiones también puede formar parte del grupo de trabajo algún auditor junior, para evitar malentendidos es conveniente definir las funciones de cada miembro del grupo de trabajo por escrito en función de sus especializaciones y experiencia aportada.

5.5 MÉTODOS, TÉCNICAS Y HERRAMIENTAS.

A lo largo de este punto hablaremos de los diferentes métodos, técnicas y herramientas utilizados actualmente para realizar auditorías informáticas.

En la actualidad podemos hablar de métodos clásicos (cuestionarios, entrevistas, observaciones, flujogramas, muestreo estadístico y memorandos) o de métodos avanzados (técnicas de concurrencia y técnicas de auditoría asistida por ordenador) que son utilizados durante el trabajo de campo para facilitar la recogida de datos.

Ahora hablaremos de los métodos clásicos; pero sin entrar en demasiado detalle.

- **Cuestionarios**: Un buen cuestionario es muy útil para cualquier auditor, el cuestionario puede ser simplemente en papel o interactivo a través del ordenador.

  A la hora de crear el cuestionario debemos tener en cuenta, si el auditor estará presente durante el mismo, que todas las preguntas sean concretas, que no estén dirigidas y evitar en la medida de lo posible las jergas.

  También debemos agrupar las preguntas por grupos o bloques que estén relacionados, un cuestionario no puede ser genérico para todas las posibles auditorías sino que debe ser específico para cada caso y deben tener un espacio en el que se puedan reflejar los datos de las personas que realiza el cuestionario y la fecha y hora.

  Podemos diferenciar distintos tipos de cuestionarios en función del tipo de respuestas, los hay simples, es decir, la respuesta se limita a sí, no o no sabe no contesta, los hay de respuesta cuantificable, es

decir, se les asigna un valor numérico y los hay de matrices, es decir, mediante matrices se representan las respuestas para accesos o validaciones de condiciones.

- **Entrevistas:** Es una reunión entre el auditor y la persona auditada, a través de la cual se recoge información muy valiosa para el informe, ya que en las entrevistas se pueden percibir situaciones o deficiencias que por otros medios no sería posible e incluso se puede atisbar la sinceridad del auditado.

  Para realizar una buena entrevista debe ser preparada concienzudamente, para ello se debe planificar y preparar específicamente para cada caso.

  A la hora de preparar la entrevista se debe tener en cuenta, el objetivo, los temas más importantes a tratar en la misma, la fecha, hora y lugar, documentarnos con la información disponible para preparar la entrevista y comprobar las funciones que deben desempeñar los entrevistados para verificar que se cumplan.

  Al realizar la entrevista debemos realizar una introducción para presentarnos, indicar la finalidad de la entrevista, la posible duración e indicar la necesidad de tomar notas para evitar malentendidos, se debe mantener un ambiente adecuado, no tener prisa por realizar la entrevista, escuchar al entrevistado y tratar de controlar el tiempo.

  En la medida de lo posible es bueno satisfacer la curiosidad del entrevistado respecto a temas generales de la entrevista.

Es importante que durante la realización de la entrevista no se intente orientar al entrevistado, evitar crear un ambiente tenso o agresivo, no dar la sensación de interrogatorio ni dar consejos.

Se debe intentar sacar el mayor jugo posible a la entrevista para ello debemos estar muy atentos a los gestos, a lo que nos estén diciendo entre líneas y si algo no nos queda claro es mejor pedir que nos lo aclaren para evitar errores.

Al final de la entrevista es conveniente hacer un resumen al entrevistado de lo que nos ha dicho para evitar errores y en lo posible dejar clara la posibilidad de una segunda entrevista para aclarar posibles puntos.

- **Observaciones:** La observación es muy importante para cualquier auditor, ya que gracias a ella se pueden detectar posibles vulnerabilidades o incumplimientos de normas, por ejemplo la puerta del CPD siempre está abierta, no es necesaria identificación para entrar,…

  También mediante la observación podemos deducir si ciertas afirmaciones que se nos hacen son ciertas o incluso podemos rebatirlas.

- **Flujogramas:** Son muy útiles para comprobar que los procedimientos, controles y autorizaciones se cumplen correctamente.

  Para ello se verifican los procesos por los que se pasa al realizar una operación, se verifica que las salidas producidas se corresponden con las entradas.

- **Muestreos estadísticos:** Son muy útiles para evitar tener que realizar un control exhaustivo de todos los datos y procesamiento de los sistemas.

  Para ello se deben elegir muestras suficientemente representativas, tanto en volumen de datos como en diversidad de los mismos, a ser posible la elección debe ser lo más aleatoria posible.

  Hay que tener cuidado a la hora de usar los muestreos ya que si no tomamos un porcentaje suficiente de datos el resultado del muestreo puede ser completamente diferente al resultado del total de los datos.

- **Comunicación escrita:** Para todo auditor es de vital importancia almacenar toda la documentación generada durante la auditoría, esta documentación suele ser de origen muy variado, como las propias notas del auditor, memorandos, correos entre los distintos miembros de la auditoría o del cliente.

  Esta información debería quedar almacenada para posibles revisiones posteriores o auditorías, por lo que es muy importante que todas las notas que se tomen puedan ser comprendidas por cualquier lector y no únicamente por la persona que realizó las anotaciones.

En la actualidad hay una gran variedad de técnicas y herramientas utilizadas durante la auditoría en función del objetivo de la misma.

A la hora de decidir usar una u otra técnica se debe tener en cuenta el soporte, la duración, el coste, la fiabilidad, compatibilidad, el tamaño de los ficheros, confidencialidad y la verificación de todo lo realizado.

Algunas de las técnicas y herramientas utilizadas por los auditores son software específico de auditoría, utilidades del software y paquetes utilizados

en los sistemas de información, todo tipo de prueba realizada sobre los datos que no afecten a los resultados reales, comprobación de los datos y procedimientos en los momentos críticos del sistema, simulaciones en paralelo y seguimientos y revisiones de los programas.

Y realizar todo tipo de simulaciones sobre los sistemas sin que estos se vean afectados, para ello se suelen utilizar los equipos de redundancia o bien para las pruebas o bien para que sigan ofreciendo los servicios que ofrecen los sistemas primarios mientras se realizan dichas pruebas.

También existen herramientas capaces de verificar que ciertos paquetes y utilidades están instalados y funcionando correctamente.

Otra técnica utilizada es la de incrustar código dentro de los procedimientos de los sistemas y lanzar los procedimientos a continuación para comprobar la traza producida, además de eliminar el código empotrado tras la prueba es fundamental que el código no afecte a la ejecución normal del sistema y en la medida de lo posible tampoco debería afectar al rendimiento del mismo.

5.6 PROGRAMA DE TRABAJO.

En el programa de trabajo se detallan los pasos necesarios a seguir para la realización de la auditoría informática, en él aparecen las áreas o departamentos de la organización que serán auditados y cómo debe hacerse.

Será utilizado por todo el equipo de trabajo, por lo que estará sujeto a continuas modificaciones.

En el programa se deben valor todos los posibles riesgos, como pueden ser: una mala gestión, vulnerabilidades, personal descontento, costes demasiado elevados,…

Se debe tener en cuenta que para obtener una mayor fiabilidad en la información recibida las fuentes tienen que ser lo más externas posibles, es decir, tendrán más fiabilidad la información que nos pueda dar un cliente de la organización que la información que nos pueda dar un jefe de sección.

A la hora de gestionar el proyecto se debe tener en cuenta las posibles prioridades del proyecto en particular, ya que en algunos casos será más importante el tiempo y en otros casos lo más importante será coste, pero en cualquier caso, siempre se debe establecer una política de mínimos que nos permita asegurar unos mínimos de calidad, duración y costes aceptables.

Para esta parte se suelen utilizar redes PERT, y herramientas de gestión de proyectos (tipo MS Project), para poder detectar tareas críticas y poder hacer asignaciones de recursos más optimas.

Para poder gestionar cualquier tipo de trabajo es necesario controlar las distintas tareas de las que está compuesto.

Habrá que identificar las distintas tareas de forma unívoca, a través de un nombre o un código, e indicar la finalidad de la misma. También es necesario

conocer la duración aproximada de la tarea, las fechas de comienzo y finalización y los recursos necesarios para llevarla a cabo.

Cada tarea tendrá un responsable y puede requerir que alguna otra tarea esté acabada antes de su comienzo. También es necesario saber que técnicas y/o herramientas se utilizarán durante su ejecución.

Toda tarea tendrá un coste asociado en función de los recursos utilizados y de su duración.

En el programa de trabajo también se deben indicar todos los costes económicos derivados de la realización de la auditoría, debidamente desglosados, indistintamente de que hagan referencia a gastos económicos por desplazamientos del equipo de auditoría (viajes, hoteles, dietas,…), como a la compra de software o hardware necesario para llevar a cabo la auditoría o incluso la contratación o colaboración de personas ajenas a la empresa que realiza la auditoría informática; pero que debido a sus conocimientos técnicos son indispensables para llevar a cabo dicha auditoría.

Es fundamental tener en cuenta que la finalidad del programa de trabajo es hallar las evidencias necesarias para poder realizar un buen informe de auditoría, estas evidencias pueden indicar que todo está correcto o graves deficiencias en algún punto de la organización; pero si se diese el caso de no hallar evidencias en ninguno de los dos sentidos, se debería replantear todo el programa de trabajo, ya que presenta alguna deficiencia grave que lo hace incorrecto, y por lo tanto no se puede aplicar para la realización de la auditoría.

5.7 EL INFORME.

El informe de auditoría no es más que una valoración de la situación actual de la organización, en la que se indican las debilidades de control interno, riesgos y posibles mejoras para solucionar dichas vulnerabilidades.

Tanto el contenido como enfoque del informe dependerán del ámbito y el objetivo marcados en la auditoría.

No se debe hacer mención a ningún nombre sino únicamente a funciones y sólo en el caso que sea estrictamente imprescindible.

La estructura del informe será similar a la siguiente, aunque no siempre tiene que ser así, ya que no hay ninguna regla concreta al respecto.

El informe debe constar de un índice, un apartado en el que se indiquen los antecedentes, otro con las conclusiones y un resumen de fácil lectura y sin términos técnicos para que pueda ser comprendido por la alta dirección sin problemas (la alta dirección suele ser la destinataria del informe), también se debe indicar en el informe el objetivo y ámbito de la auditoría, así como el período de tiempo. También se deben indicar los agradecimientos en el informe, siempre y cuando procedan.

También es necesario indicar el entorno informático y las posibles limitaciones.

Una vez descrita la estructura del informe hablaremos del contenido.

El informe se puede estructurar por los tipos de control e ir indicando cuales de los mismos se implementan en la organización y si dicha implementación es correcta, cuáles de estos controles no son necesarios y qué controles que son necesarios no aparecen. Pero suele ser más conveniente organizar el informe por áreas, ya que de esta forma es más fácil para la organización saber qué

áreas debe reforzar en mayor medida o en cuales debe hacer reestructuraciones para que sean más eficientes.

Es conveniente que a la hora de realizar el informe se trate de agrupar los puntos homogéneos, ya que cada punto debe incluir la descripción de la deficiencia o vulnerabilidad, la probable causa de la misma, cuál es el posible efecto que puede producir sobre la organización e incluir la recomendación en la que se debe indicar cuál es la mejor forma de solucionar la deficiencia y por qué esa es la mejor manera de solventar el problema y no otra.

Es conveniente que en el informe se indiquen qué vulnerabilidades son las más críticas dentro de cada área, una buena forma de realizarlo es indicar junto a cada deficiencia su prioridad relativa, es decir, en una lista de prioridades de 0 a 10 el 0 sería la menos prioritaria de todas y el 10 la más prioritaria.

También es conveniente indicar el nivel de riesgo de cada vulnerabilidad (aunque con las prioridades quede más o menos claro siempre es mejor asegurar) y un posible plazo de implantación máximo de la posible solución y por último se debe indicar el esfuerzo y coste aproximado de la implantación.

Aunque no es obligatorio es muy conveniente incluir varios anexos en los que se reflejen las distintas entrevistas y cuestionarios, así como toda la documentación utilizada durante el proceso de auditoría.

Es recomendable que el informe entregado este protegido de alguna manera para que no pueda ser modificado con posterioridad, además es conveniente que todas las páginas estén numeradas y con encabezados y pies de página.

También se puede incluir la palabra CONFIDENCIAL como marca de agua en todas las páginas o en el caso del borrador la palabra BORRADOR y que aparezcan las firmas de los auditores en todas las páginas.

En el caso de que se entreguen más de una copia del informe, se podría diferencia cada copia con un código de barras o con el nombre del destinatario.

Lo que se intenta obtener con todas estas medidas es el primer lugar que el informe no pueda ser modificado o manipulado por nadie, y que en el caso de que se hiciera público total o parcialmente poder saber qué persona o personas son las que han hecho público el informe.

Es conveniente realizar un borrador del informe de auditoría para que en primer lugar sea discutido por todos los miembros del grupo de trabajo y una vez obtenido un consenso entre los miembros del grupo de trabajo se entregaría el borrador a los auditados para de esta forma evitar malentendidos.

Normalmente se discute el contenido del borrador entre los auditados y los auditores, en esta reunión los auditores presentan todas las evidencias en las que se sustentan sus afirmaciones y se trata de llegar a un consenso entre ambas partes, en ocasiones se acuerda modificar algún párrafo, pero sin restarle veracidad. Este proceso es necesario para poder presentar el informe definitivo, ya que sobre el informe definitivo no cabe ninguna modificación posterior.

El informe definitivo se entrega a la persona o entidad que lo encargo y se suele acompañar de un acuse de recibo.

Es conveniente recordar que las recomendaciones indicadas en el informe en ningún caso son vinculantes y siempre es la organización la que debe decidir si lleva a cabo todas las recomendaciones, sólo las más críticas o si por el contrario decide no implementar ninguna.

5.8 AUDITORÍA DE LA SEGURIDAD.

Hemos creído necesario incluir este punto, ya que el tema principal del presente proyecto final de carrera es la auditoría de la seguridad, para que cualquier persona que lea nuestro proyecto final de carrera, y no sea ningún experto informático ni en seguridad ni en auditoría informática, pueda comprender perfectamente el significado y el espíritu del presente proyecto final de carrera.

Antes de realizar una auditoría de seguridad hay que tener en cuenta si los posibles riesgos son conocidos, si se tiene apoyo de los distintos comités de seguridad, cuál será el objetivo, el ámbito y la profundidad de la auditoría. Si existen algún tipo de plan o política de seguridad y qué procedimientos de seguridad existen. Cuál es la inversión en seguridad de la organización y si es suficiente. Comprobar que los controles de seguridad existentes son suficientes. Es necesario conocer quiénes son los responsables y quienes los propietarios de la información en los sistemas de información de la organización.

También es necesario conocer en detalle la estructura informática de la organización para comprobar si los datos y los programas están separados entre sí.

Se debe comprobar la existencia de auditorías anteriores tanto internas como externas

Se debe comprobar quiénes son los responsables de la seguridad de la organización y si se toman medidas tanto para asegurar la seguridad física como lógica de los sistemas.

A la hora de realizar una auditoría de la seguridad siempre se deben tener muy presentes la disponibilidad, la integridad, la confidencialidad, la autenticación y el no repudio de los datos almacenados y procesados por los sistemas de información de la organización.

Es fundamental conocer los posibles riesgos que pueden afectar a los sistemas, ya que debido al crecimiento tecnológico actual de la informática y las telecomunicaciones, los sistemas y tecnologías utilizados por las organizaciones cada vez son más complejos y costosos, y por lo tanto son más complicados de administrar y de proteger.

Los riesgos a los que se encuentran expuestos los sistemas son muy variados, pueden ir desde errores o delitos hasta cualquier tipo de desastre natural pasando por virus, ataques y averías.

En función de la magnitud del riesgo al que se haya visto sometido una organización puede incluso llegar a desaparecer, ya sea porque el defecto ha producido graves pérdidas, o incluso por requerimiento judicial por no cumplir alguna directiva legal vigente aplicable al ámbito de la organización.

Para poder realizar una auditoría de seguridad es fundamental implicar a todos los estamentos del organigrama de la organización, es decir, deben colaborar en la auditoría desde la dirección general hasta los usuarios de los sistemas de información de la organización pasando por los distintos estamentos del organigrama.

Es de vital importancia que todo el servicio o departamento de seguridad este comprometido con la auditoría, al igual que los auditores internos y externos. También es conveniente evaluar las relaciones y comunicaciones con las empresas prestadoras de servicios.

Por lo tanto, para poder realizar una auditoría de seguridad es necesaria la colaboración de los responsables de informática y de seguridad de la organización, que se revisen todos los planes de seguridad y de funciones.

Es necesario revisar las funciones y responsabilidades de todos los miembros de la organización y evaluar el grado de motivación de los mismos para intentar hallar posibles empleados descontentos que en un futuro puedan llegar a realizar acciones perjudiciales para la organización.

Hay que comprobar la seguridad de todas las comunicaciones, la seguridad jurídica y organizativa, la seguridad de programas y de datos, la seguridad física y lógica y por último revisar los distintos planes de contingencia.

Es muy conveniente, por no decir vital, que en toda organización haya un departamento encargado de la administración de la seguridad, este departamento sólo ha de depender de la alta dirección y ha de ser independiente del resto de servicios o áreas para asegurar su correcto funcionamiento.

Es responsabilidad de los administradores de seguridad conocer toda la legalidad y políticas aplicables a la organización y en función de las mismas elaborar planes y procedimientos, también deben encargarse de proteger todos los recursos de la organización ya sean informáticos o de cualquier otro tipo, como puedan ser sus infraestructuras.

La administración de seguridad debe comprobar posibles irregularidades y o bien subsanarlas o ponerse en contacto con los responsables para que las solucionen. Otro de sus cometidos es dar soporte a los distintos departamentos o áreas de la organización en cuanto a temas de seguridad se refiere.

También pueden recomendar que se lleven a cabo auditorías tanto internas como externas, para asegurar una seguridad mayor de la organización.

Dentro de seguridad se pueden distinguir entre dos tipos de seguridad, la seguridad lógica y la seguridad física, aunque ambas deben depender siempre del grupo de seguridad, dependiendo de las organizaciones las mismas personas pueden realizar las tareas de ambas o puede haber un grupo dedicado exclusivamente a la seguridad lógica y otro a la seguridad física, ya que en la actualidad tampoco existe ninguna normativa que regule que personas pueden desempeñar cada una.

- **Seguridad física:** Se centra especialmente en la ubicación de los sistemas de información, estudia el terreno donde se van a alojar los sistemas de información para evitar posibles desastres naturales (terremotos, riadas,..), desastres derivados de la intervención del hombre (rutas aéreas, curvas de carreteras,…) y es muy importante que no se indique la localización exacta de los sistemas de información para evitar posibles intentos de acceso físico a los sistemas.

  Se encarga de realizar todas las comprobaciones de protecciones externas como pueden ser: detectores de movimiento, de sonido, arcos detectores, escaneo de correo postal, identificación para acceder a los edificios, vigilantes de seguridad,…

  También se encarga de comprobar los controles del entorno como pueden ser: alarmas de fuego, climatización adecuada, botiquines,…

  Es muy conveniente que las diferentes áreas se encuentren separadas, es decir, que el desarrollo y la producción no se realicen

en el mismo sitio, que las operaciones sobre los sistemas se hagan por consola remota y no delante del terminal(siempre que sea posible),..

La seguridad física se centra sobre todo en tres aspectos cruciales y que afectan seriamente a las máquinas de los sistemas de información como son el fuego, el agua y los suministros eléctricos.

Para el fuego es necesario tener sistemas de detección y de extinción lo más eficientes posibles y que dañen lo mínimo posible a las máquinas, también es conveniente la existencia de armarios ignífugos y de señales de tomas de aguar para los bomberos.

Para el agua es necesario tener sistemas de detección del grado de humedad, es conveniente que la sala en la que se encuentre las máquinas este por encima del nivel de la calle o si no al menos al mismo nivel para evitar inundaciones, que las acometidas de agua estén por debajo de las máquinas, que existan drenajes, que existan fundas protectoras para tapar los equipos en caso necesario.

Para los suministros de electricidad es conveniente tener redundancia en el suministro de diferentes proveedores y si es posible de distintas centrales, que existan grupos electrógenos y sistemas de alimentación ininterrumpida, que la instalación eléctrica esté protegida y que los distintos entornos (climatización, alarmas, controles y máquinas) estén alimentados desde varias fuentes y que los distintos entornos no compartan fuentes de alimentación.

- **Seguridad lógica:** Se centra especialmente en los métodos de autenticación, podemos dividir los métodos de autenticación en

aquellos que se basan en una característica identificativa de cada persona (huella dactilar, retina,…), en aquellos que se basan en una posesión propia de cada individuo (tarjeta magnética, DNI,…), aquellos que se basan en algo que sólo conocen los individuos autorizados (contraseñas, cifrado) y aquellos que se basan en una actividad que se es capaz de realizar (firma).

Uno de los principales aspectos de la seguridad lógica son las contraseñas, la asignación de contraseñas es un tema bastante delicado, pero indistintamente de quién o qué proceso nos asigne la contraseña, es mucho más importante que esa contraseña sólo sea de activación, y que una vez dentro de los sistemas, el usuario este obligado en primer lugar a cambiar su contraseña antes de realizar ninguna otra operación.

Una buena contraseña debe ser fácil de recordar pero también tiene que ser difícil de adivinar por terceras personas, es muy recomendable que no represente ninguna palabra del alfabeto, que contenga caracteres alfanuméricos y que tenga una longitud entre 8 y 10 caracteres.

Es muy importante que ningún usuario facilite su contraseña a otra persona.

Al introducir la contraseña en el sistema para acceder al mismo, la contraseña no debería aparecer visible en la pantalla.

Dentro de los sistemas las contraseñas deberían almacenarse cifradas, para que nadie pueda tener acceso a las contraseñas de otros usuarios.

Para realizar una buena gestión de contraseñas, se debería establecer una caducidad periódica de las contraseñas y que no se permitiese a los usuarios introducir su misma contraseña o modificada sólo en un carácter cada vez que la contraseña caducase, tampoco se debería permitir rellenar el número mínimos de caracteres con algún carácter repetido al final, es muy recomendable que las contraseñas sean distribuidas por canales seguros para que no puedan ser interceptadas por terceros.

Otro de los aspectos fundamentales de la seguridad lógica es el cifrado de la información, que no desarrollaremos a lo largo de este apartado, ya que consideramos que a lo largo del presente proyecto final de carrera se ha visto con la suficiente profundidad.

En la actualidad la firma electrónica ocupa un papel destacado en la seguridad lógica, principalmente porque es muy fácil de producir y de comprobar su autenticidad, en teoría es infalsificable y su propietario no puede rechazar su validez, aunque puede intentar rechazar su autoría alegando cualquier tipo de ataque sobre el sistema en el que estaba almacenada su firma electrónica.

En los sistemas operativos es conveniente conocer a las personas que los instalaron y saber si lo hicieron siguiendo algún procedimiento y cuál, deben almacenar en el fichero de log todas las conexiones, que el acceso remoto este limitado tanto por usuarios como por direcciones IP, que los usuarios tengan limitado el acceso al sistema en función de sus distintos perfiles.

5.9 AUDITORÍA DE LA SEGURIDAD EN APLICACIONES.

Hemos decidido incluir este punto en la memoria del presente proyecto final de carrera, porque creemos interesante dar una visión, aunque sea de forma muy general, de cómo debería hacerse una auditoría de seguridad en aplicaciones, creemos que es interesante porque forma parte del tema del presente proyecto final de carrera, en el siguiente punto del proyecto fin de carrera aplicaremos lo expuesto en este punto y en todos los demás de las memoria para realizar una auditoría de seguridad de Lotus Notes

Las auditorías de seguridad en aplicaciones son de vital importancia para poder certificar que las aplicaciones realizadas por la organización son seguras y que por lo tanto se pueden utilizar para uso interno de la organización y/o para comercializar dichas aplicaciones.

Una buena auditoría de seguridad en aplicaciones evita muchos problemas de fraude e incluso errores de programación; pero para esto se deben seguir una serie de pautas de programación estructurada al desarrollar las aplicaciones (ciclos de vida, separación de entornos, encapsulación de datos,…).

Se deben evaluar todos los riesgos potenciales durante el desarrollo de las aplicaciones, en función de los entornos y tecnologías utilizados, la metodología y herramientas usadas en el proceso de auditoría, el número de puntos función, perfiles del jefe de proyecto y de los analistas y programadores, duración del proyecto y de la calidad.

Se deben controlar todas las entradas de la aplicación, los ficheros utilizados, las interrelaciones con otras aplicaciones y/o procesos, que se produzcan los mensajes de alerta o informes de excepción en los casos que se produzcan errores o situaciones anómalas.

Se deben realizar las pruebas necesarias que contemplen todas las situaciones posibles y verificar que durante la ejecución se realizan todas las rutinas pertinentes. Estas pruebas se pueden realizar con copias de datos reales, siempre que los datos no sean de acceso protegido o restringido.

Una vez que se ha implantado la aplicación esta puede ser modificada, y dichas modificaciones podrían generar nuevas vulnerabilidades sobre la aplicación, por lo que estas nuevas modificaciones deben ser comprobadas de igual forma que el resto de la aplicación, pero además antes de comenzar a realizar las modificaciones se deben realizar análisis de impacto y planes de implantación de dichas modificaciones.

5.10AUDITORÍA DE LA SEGURIDAD EN COMUNICACIONES.

Hemos creído necesario incluir este punto en la memoria del actual proyecto final de carrera, aunque no forme parte del tema principal del proyecto de forma directa sí lo hace forma indirecta, puesto que el tema del proyecto final de carrera es la auditoría de seguridad de Lotus Notes, que al tratarse de un gestor de correo electrónico está muy ligado a internet y por lo tanto a las comunicaciones.

Se deben proteger las comunicaciones tanto de forma lógica como física, es decir, es necesario comprobar la seguridad de todos los terminales y nodos, así como la de todas las transacciones y programas utilizados.

Se debe intentar asegurar en todo momento la disponibilidad de los sistemas a través de la red, este suele ser un tema complicado ya que no solo depende de la administración de los equipos propios sino también depende de que los suministradores de servicios puedan garantizar un servicio ininterrumpido, para poder solventar este tipo de problemas es conveniente tener duplicidad en todos los controles de comunicaciones y distintos suministradores de servicios. También es de vital importancia poder asegurar la confidencialidad y la integridad de la comunicación, mediantes sistemas de cifrado.

Se debe controlar el acceso a los terminales de los sistemas mediante usuario y contraseña, almacenar las conexiones a los mismos y los intentos de conexión, desconexión de usuarios inactivos, suspensión de la comunicación tras n intentos de conexión consecutivos fallidos.

Debido al gran incremento de las operaciones realizadas a través de internet, como realizar compras en línea, consultar saldos de cuentas bancarias, domiciliaciones de recibos,… es necesario crear una estructura de comunicaciones más segura y robustas, que eviten en la medida de lo posible cualquier ataque o vulnerabilidad del sistema, entre estas medidas pueden destacarse los cortafuegos y el cifrado de todas las comunicaciones.

Además todas estas transacciones no se realizan únicamente a través de ordenadores domésticos, sino que también se realizan a través de móviles, PDAs, terminales de pago, cajeros automáticos,... por lo que la administración de las comunicaciones se hace todavía más compleja.

Teniendo en cuenta la naturaleza de las operaciones citadas anteriormente es fundamental asegurar la seguridad, ya que de no ser así los datos bancarios de las personas que utilizaron estos servicios podrían verse expuestos de tal forma que una tercera persona podría tener acceso a dichos datos y utilizarlos en beneficio propio.

5.11AUDITORÍA DE LA SEGURIDAD EN EL CORREO ELECTRÓNICO.

A lo largo de este apartado trataremos de dar una visión completa de lo que debería ser la seguridad en el correo electrónico, para ello, nos basaremos especialmente en el Título VIII del Reglamento de desarrollo de la ley orgánica de protección de datos de carácter personal, en la ley de servicios de la sociedad de la información y de comercio electrónico, ambas leyes han sido vistas con el suficiente detalle a lo largo del punto 4 del actual proyecto final de carrera, y en el estándar ISO 27002 sobre seguridad informática, que será visto con el suficiente detalle a lo largo del anexo a.

Indicaremos cuáles deben ser los puntos tomados en consideración por las distintas organizaciones, para que sus sistemas de correo electrónico se puedan considerar seguros.

También indicaremos de qué tipo deben ser las políticas internas de las organizaciones en relación con el correo electrónico y el uso tanto por parte de los empleados como por parte de la alta dirección de las mismas.

Es conveniente que destaquemos que las medidas de seguridad y políticas mencionadas a lo largo de este apartado son genéricas, y deberían ser útiles para todo sistema de correo electrónico, indistintamente de cuál sea la tecnología utilizada. Por este motivo, a lo largo de este punto no mencionaremos en ningún momento la aplicación Lotus Notes.

Los puntos que se deben comprobar en un sistema de correo electrónico están ampliamente relacionados con los equipos que forman parte del sistema de correo electrónico, es decir, con los servidores de correo, los servidores de

red, los equipos de redundancia y de alta disponibilidad, sistemas de copias de seguridad y las aplicaciones de correo electrónico, por lo tanto, los puntos que se deben evaluar formaran parte de alguno de estos cinco elementos.

En primer lugar empezaremos por los puntos que se deben evaluar dentro de los servidores de correo electrónico:

- Se debe comprobar que el número de estafetas de correo o MTAs es suficiente para soportar la carga del sistema, es decir, debemos verificar que en ningún momento los correos enviados o recibidos se pierden debido a que los servidores de correo está saturados y no pueden ofrecer sus servicios.
- Se debe comprobar que únicamente los administradores de los servidores de correo tienen acceso a los mismos, y que el resto de miembros de la organización no tengan acceso a los servidores.
- Los usuarios de correo electrónico sólo han de poder acceder al correo almacenado en su buzón y no al del resto de usuarios del sistema.
- El acceso a los servidores de correo electrónico ha de estar controlado, y en la medida de lo posible, se ha de limitar la forma de acceso a los mismos por parte de los administradores, es decir, sólo se ha de poder acceder a ellos por consola, desde unas ips específicas, etcétera.
- Se debe comprobar la existencia de servidores antispam que eviten que los usuarios reciban correos electrónicos no deseados y de escasa utilidad.

- Se debe verificar que todos los servidores de correo estén debidamente actualizados y que tengan instaladas las últimas versiones, o las más estables, de todos los paquetes de software instalados en los servidores.

En segundo lugar indicaremos los puntos que se deben evaluar en los servidores de red vinculados al sistema de correo electrónico:

- Se debe comprobar la existencia de cortafuegos en los servidores de red, que eviten accesos de personas externas a la organización.
- Se debe comprobar que existan utilidades de antivirus que eviten que usuarios externos a la organización tengan acceso a los servidores e incluso puedan tomar modificar total o parcialmente su configuración.
- Se debe comprobar que únicamente los administradores de los servidores de red tienen acceso a los mismos.
- Se debe comprobar que el acceso a los servidores está limitado y controlado, es decir, sólo se podrá acceder a los servidores de red desde la consola de los propios servidores, desde una IP determinada, etcétera.
- Los servidores de red deben estar debidamente actualizados y las últimas versiones, o las más estables, de los paquetes de seguridad.

En siguiente lugar indicaremos los puntos que se deben estudiar en los sistemas de redundancia y de alta disponibilidad:

- Se debe comprobar que todos los servidores dispongan de varias fuentes de alimentación, que eviten que el equipo quede sin alimentación eléctrica en el caso que se produjese una avería.
- Se debe comprobar que las fuentes de alimentación de los servidores estén conectadas a diferentes circuitos eléctricos que eviten la caída de los servidores en el caso que se produjese cualquier problema en uno de los circuitos eléctricos.
- Se debe comprobar que el suministro eléctrico sea de diferentes centrales eléctricas, para asegurar un suministro permanente de corriente eléctrica.
- Se debe comprobar la existencia de sistemas de alimentación ininterrumpidos, que permitan a los servidores seguir encendidos aunque el suministro eléctrico se corte temporalmente por algún motivo.
- Se debe comprobar si existe algún tipo de acuerdo con alguna otra organización, por el cual se encolen todos los correos electrónicos destinados a la organización, en el caso que los servidores de correo no estuviese operativos, para de esta forma no perder ningún correo destinado a la organización.

Ahora indicaremos los puntos que se deben estudiar dentro de los sistemas de copias de seguridad:

- Se debe comprobar que todos los servidores que intervienen en el sistema de correo electrónico realicen copias de seguridad tanto del sistema operativo como de los datos alojados en los mismos.

- Se debe comprobar que sólo los administradores de los sistemas de copias de seguridad tienen acceso a todas las copias de seguridad de los diferentes servidores de la organización.
- Se debe comprobar que sólo los administradores de los servidores, además de los administradores de los sistemas de copias de seguridad, tienen acceso a las copias de seguridad de sus servidores.
- Se debe comprobar que sólo los administradores de los sistemas de copias de seguridad tienen acceso a los mismos.
- Se debe comprobar que únicamente se pueda acceder a los sistemas de copias de seguridad en la forma indicada, es decir, sólo serán accesibles por consola, desde determinadas ips, etcétera.
- Se debe comprobar que los sistemas de copias de seguridad estén actualizados con la última versión de los paquetes de software instalados o la versión más estable de los mismos.

Por último indicaremos los puntos que se deben evaluar dentro de las aplicaciones de correo electrónico:

- Los usuarios de las aplicaciones de correo sólo han de poder acceder a las mismas en la forma indicada, es decir, para acceder a las mismas se ha utilizar un gestor de correo electrónico de escritorio, un webmail, etcétera.
- Los distintos usuarios únicamente han de tener acceso a la información asociada a su usuario, y por lo tanto, ningún usuario ha de poder acceder a la información de otro.

- Se debe comprobar que sólo los administradores de las aplicaciones de correo electrónico tengan acceso a la información almacenada en las aplicaciones de correo electrónico.
- Se debe comprobar que la información almacenada en las aplicaciones de correo electrónico se encuentra debidamente cifrada, y que dicho cifrado es acorde con la información protegida.
- Se debe comprobar que las distintas aplicaciones de correo electrónico se encuentran debidamente actualizadas con las últimas versiones de software o con las más estables teniendo en cuentas las distintas características de las aplicaciones de correo electrónico.

Las políticas internas que se deben evaluar en relación con los sistemas de correo electrónico, son todas aquellas políticas que estén relacionados con el comportamiento de los miembros de la organización en la administración o utilización de alguno de los equipos que intervienen en el sistema de correo electrónico de la organización.

Entre las políticas que se deben evaluar podemos destacar todas aquellas que hagan referencia al modo de acceso tanto a los servidores como a las aplicaciones que estén relacionadas con el sistema de correo electrónico.

También es necesario evaluar todas aquellas políticas en las que se indique cuál debe ser el vocabulario utilizado por el personal de la organización en el envío y contestación de correos electrónicos, indistintamente del tipo de correo electrónico.

Se debe evaluar toda aquella política en la que se reflejen las normas de uso del correo electrónico interno de la organización, es decir, se autoriza o no el uso del correo electrónico interno para utilización personal.

Se debe evaluar toda aquella política que refleje que tipo de uso está permitido para todos los equipos informáticos y aplicaciones relacionados con el sistema de correo electrónico.

Se debe evaluar toda aquella política que haga mención a la utilización por parte del personal de la organización de material privado, en relación con los sistemas vinculados al correo electrónico.

Se debe evaluar toda política que indique el tratamiento que se debe dar a las copias de los correos enviados y recibidos, es decir, en qué forma y manera se deben guardar o eliminar los correos electrónicos pertenecientes a la organización.

6. ESTUDIO DE LOTUS NOTES.

6.1 INTRODUCCIÓN.

A lo largo de este punto mencionaremos las acciones necesarias para crear un informe de auditoría desde el punto de vista de la seguridad del programa Lotus Notes, que es el objetivo final del actual proyecto fin de carrera, ya que como comentaremos a continuación, nos es imposible realizar tanto una auditoría informática desde el punto de vista de la seguridad de la aplicación Lotus Notes, como el informe de auditoría vinculado a la propia auditoría.

Para la elaboración de este punto hay varias aspectos que debemos tener muy presentes durante toda la preparación y elaboración, ya que sin esta aclaración podrían producirse malentendidos de la finalidad y alcance del mismo:

- En primer lugar, tenemos que tener en cuenta que como no trabajaremos con la aplicación instalada sobre los equipos de una organización, no dispondremos de ninguna normativa interna que deba cumplir la instalación y configuración de la aplicación, por lo tanto, nos hemos visto obligados a suponer cuales son los posibles elementos de riesgo y estudiarlos, para ello nos hemos guiado por el estándar ISO 27002 y por nuestra propia experiencia, por este motivo debemos nombrar las distintas políticas que debería cumplir la instalación y configuración de la aplicación en cualquier organización.

  Por este mismo motivo tampoco dispondremos de ningún control interno que deba cumplir la instalación y configuración de la

aplicación, en este caso también nombraremos los posibles controles que deberían estar implementados para asegurar la instalación y configuración de la aplicación.

- En segundo lugar, tenemos que tener en cuenta toda la normativa legal vigente que pueda ser aplicada durante el uso de la aplicación, y estudiar qué configuración de los distintos parámetros de la configuración de la aplicación es la correcta para cumplir con toda la normativa legal y evitar posibles acciones legales en contra de la organización.

  Como no disponemos de ninguna organización no podemos comprobar que la organización haya tenido en cuenta la normativa legal a la hora de configurar la aplicación, por lo que sólo podremos indicar qué parámetros de la aplicación son los correctos para evitar posibles acciones legales en contra de la organización.

- En tercer lugar, tenemos que tener en cuenta que debido a que no disponemos de una organización tampoco disponemos del personal de la organización, para poder entrevistarnos con ellos, y sacar nuestras propias conclusiones respecto a qué medidas que dependen de la cooperación del personal para que se lleven a cabo correctamente.

  Pero lo que si podemos es llevar a cabo los diferentes cuestionarios que se deberían realizar a los distintos empleados de la organización en función de sus funciones y responsabilidades, ya que aunque un gran número de preguntas de los cuestionarios pueden ser comunes para todos los empleados, habrá otras preguntas que serán

específicas dependiendo del perfil del entrevistado y sobre todo de sus funciones y responsabilidades.

- En cuarto lugar, tenemos que tener en cuenta que no será necesario desarrollar un programa de trabajo completo con planificaciones de trabajo, entrevistas, etcétera, ya que como hemos mencionado anteriormente al no tener empleados a los que entrevistar, no será necesario planificar la duración de las entrevistas, seleccionar a los empleados a los que entrevistar ni el orden de las mismas.

  Por este mismo motivo, tampoco será necesario realizar la planificación de las distintas reuniones y entrevistas con los departamentos y áreas para solicitar el acceso a la información necesaria o en su caso llegar a un acuerdo de qué datos serán accesibles y cuáles no.

  Por descontado, que tampoco será necesario planificar las distintas reuniones y entrevistas con la alta dirección o con el departamento o sección que hubiese encargado nuestra auditoría para solicitar el acceso a la normativa de la empresa y posteriormente presentarles el borrador de auditoría y por último el informe de la auditoría.

- Por último, tenemos que tener en cuenta que el informe final de auditoría, no será un informe al uso, ya que como comentamos en el punto 5 del presente proyecto final de carrera el objetivo principal de un informe de auditoría es evaluar el estado actual de una organización en relación a sus sistemas de información; pero en nuestro caso este no será el objetivo de nuestro proyecto final de carrera sino que a lo largo de este punto intentaremos reflejar cuál

debería ser la configuración más apropiada de la aplicación Lotus Notes y que mecanismos suplementarios deberían estar implementados para asegurar que la configuración cumple con la legislación vigente y que además desde el punto de vista de la seguridad informática, la instalación y la configuración son correctas.

El ámbito de la auditoría como hemos ido comentando tampoco será el normal de una auditoría, ya que se limitará exclusivamente a la evaluación de las distintas opciones de configuración de una versión de evaluación de la aplicación Lotus Notes sobre un ordenador de sobremesa, usaremos una versión de evaluación porque la aplicación Lotus Notes no está disponible en versiones completas gratuitas y teniendo en cuenta que la finalidad del proyecto era realizar una auditoría y no una evaluación crítica y completa del programa no hemos creído necesario comprar una licencia completa sólo para verificar que ciertas opciones, que no están incluidas en la versión de evaluación, y que por lo tanto no hemos podido comprobar funcionan tal y como especifica el fabricante.

6.2 EVALUACIÓN DE RIESGOS.

Para poder evaluar de forma correcta los riesgos de cualquier sistema en primer lugar debemos estudiar las posibles vulnerabilidades del sistema y a continuación comprobar que los distintos controles internos implementados por la organización y que la implementación de las distintas políticas internas evitan las posibles vulnerabilidades del sistema descubiertas con anterioridad.

En nuestro caso, como hemos comentado en el punto anterior, no disponemos de ningún control interno implementado por la organización ni política interna, por lo que en este punto además de enumerar las posibles vulnerabilidades de la aplicación Lotus Notes, también comentaremos de forma general en qué deberían consistir los diferentes controles internos encargados de solventar las distintas vulnerabilidades y las políticas internas en las que se deben recoger los controles.

En primer lugar vamos a enumerar las distintas vulnerabilidades a las que puede estar sometida la aplicación Lotus Notes.

1.- El acceso a la aplicación Lotus Notes sólo debe estar permitido a las personas autorizadas a utilizar el programa y cada una de ellas debe tener su propia cuenta independiente del resto, es decir, que no debe haber cuentas genéricas de correo electrónico que sean utilizada por todo el personal de la organización o por todos los miembros de un grupo o departamento.

2.- En el caso que varios usuarios compartan equipo o que más de un empleado de la organización pueda acceder al mismo equipo, se debe configurar la aplicación Lotus Notes para que cada vez que se inicie, solicite usuario y contraseña, también será necesario que los equipos en

los que esté instalada la aplicación Lotus Notes soliciten usuario y contraseña para iniciar sesión en el mismo.

De esta forma se evita que personas no autorizadas accedan al programa y tengan acceso a los correos enviados y recibidos así como al resto de información privada almacenada en la aplicación Lotus Notes.

3.- En relación con el anterior riesgo también es recomendable que sólo el personal autorizado tenga acceso a la sala en la que se encuentren los equipos en los que está instalada la aplicación Lotus Notes, ya sea mediante tarjetas de acceso a esa sala, al edificio o mediante cualquier otro tipo de control de acceso biométrico o a través de vigilantes de seguridad, para la identificación manual de todas las personas que entren en la sala y/o en el edificio.

4.- La configuración de la aplicación Lotus Notes debe permitir que la aplicación se bloquee de forma automática por inactividad, de esta forma se evita que si un usuario tiene abierta la aplicación Lotus Notes y por algún motivo debe abandonar su equipo y se olvida de cerrar o de bloquear la aplicación Lotus Notes, otra persona utilice la aplicación Lotus Notes con un usuario que no le corresponda, con lo que tendría acceso a los correos y la libreta de direcciones de otro usuario de la aplicación Lotus Notes, por lo que podría eliminar cualquier correo, realizar cualquier modificación sobre la libreta de direcciones o enviar correos electrónicos con la identidad de otro usuario.

Sería muy recomendable que la organización tuviese alguna política de seguridad en la que se indicase el tiempo máximo que puede quedar la

aplicación Lotus Notes desatendida, trascurrido el mismo la aplicación Lotus Notes debería bloquearse de forma automática.

5.- También es muy recomendable que los equipos informáticos tengan activado el auto bloqueo por inactividad, para evitar que cualquier otra persona pueda acceder al equipo informático sin identificarse y hacerse pasar por otro usuario.

Al igual que en el caso anterior, es muy recomendable que la organización tenga alguna política de seguridad en la que se indique el tiempo máximo que puede estar un equipo informático desatendido, trascurrido el cual el equipo informático debería bloquearse de forma automática.

6.- Sería muy interesante que la organización dispusiera de una política de cambio de claves de forma periódica, tanto de acceso a los equipos informáticos como de acceso a la aplicación Lotus Notes y en la medida de sus posibilidades debería implementar algún tipo de control para verificar que dichos cambios de contraseñas se realizan en el plazo y forma estipulados en la política interna definida por la organización, siempre para los equipos informáticos, ya que como comentaremos más adelante la aplicación Lotus Notes permite la caducidad de las contraseñas de acceso.

7.- Aunque el acceso a la aplicación Lotus Notes y a los equipos informáticos, en los que esté instalada la aplicación, esté restringido sólo a las personas que están autorizadas a utilizar la aplicación, se debe tener especial cuidado con la privacidad de la libreta de direcciones de los distintos usuarios, ya que si varios usuarios comparten el mismo equipo

informático y además tienen acceso a la aplicación Lotus Notes, podrían tener acceso a la libreta de direcciones del resto de usuarios del equipo informático.

Por lo tanto, es necesario que las libretas de direcciones de los diferentes usuarios estén codificadas y sólo sean accesibles por sus respectivos propietarios, de esta forma se evita que los diferentes usuarios tengan acceso a los datos privados de los contactos del resto de usuarios de la aplicación Lotus Notes, ya que si tuviesen acceso a los datos personales de los contactos del resto de usuarios se podría considerar que se vulnera la ley orgánica de protección de datos de carácter personal, ya que en la libreta de direcciones de la aplicación Lotus Notes se pueden reflejar diferentes datos de los contactos como son: nombre, apellidos, dirección, teléfono, etcétera que son considerados datos de carácter personal, debido a esto es muy conveniente que la organización tenga alguna política interna en la que se refleje esta situación y se indique que lo más conveniente para todas las instalaciones de la aplicación Lotus Notes tengan activa esta opción.

8.- Como comentamos a lo largo del punto 4 en el apartado sobre la LOPD los archivos temporales que se crean para trabajar con datos deben ser eliminados tras la realización del trabajo para el que surgió la necesidad de crearlos, ya que si dichos archivos temporales son almacenados, cualquier persona que tuviese acceso al equipo podría tener acceso a los datos temporales. La aplicación Lotus Notes también crea ficheros temporales al enviar correos, adjuntar ficheros, al modificar la libreta de direcciones,.. Por lo que la aplicación Lotus Notes debería

eliminar todos los archivos temporales que haya creado durante su utilización cuándo deje de necesitarlos o al cerrar la aplicación; para que de esta forma ningún usuario pudiese tener acceso a los datos contenidos en esos archivos temporales, aunque ocasionalmente, se producen fallos en la eliminación automática de estos ficheros temporales.

Es muy conveniente que la organización defina alguna política interna en la que se recoja esta problemática y se indique la importancia de la eliminación de los archivos temporales y se indique el plazo de eliminación y la forma en la que se deben borrar dichos ficheros.

9.- Uno de los principales problemas del envío de correo electrónico es conseguir la autenticación del remitente del correo electrónico, en la actualidad es técnicamente imposible asegurar que todos los correos que recibimos pertenecen al destinatario que aparece en el mismo.

En la actualidad es posible firmar los correos electrónicos que enviamos mediante firma electrónica, lo que permite asegurar la autoría de los mensajes recibidos en esta forma.

La aplicación Lotus Notes permite la firma de correos electrónicos mediante firma digital o electrónica, lo que permite a los receptores de los correos verificar que el remitente es quién dice ser, aunque esta medida no es obligatoria, sí que es muy recomendable para cualquier organización ya que los receptores de los mensajes podrán estar seguros de que el emisor del correo recibido es quién dice ser.

La organización debería definir alguna política interna que recoja la conveniencia para la organización de implementar esta opción.

10.- Otro de los problemas del envío de correo electrónico es poder asegurar que el contenido del mensaje no se ha visto modificado desde que se envío hasta que llego al receptor.

Aunque actualmente se han desarrollado soluciones parciales como son el envío de correo seguro a través de SSL que aseguran que los correos enviados a través de este protocolo no pueden haber sido modificados, gracias a que se pueden enviar de forma cifrada lo que asegura que los mensajes no pueden haber sido modificados desde que el emisor los envía hasta que el receptor de los mensajes los recibe.

Al igual que en el caso anterior la aplicación Lotus Notes permite el envío de correos en forma segura, pero esta medida tampoco es obligatoria, pero igualmente es muy recomendable para cualquier organización ya que los receptores de los mensajes sabrán que el mensaje no puede haber sido alterado desde que se envío hasta que ellos lo recibieron, por lo que su contenido es el original.

La organización debería implementar las políticas internas que estimase oportunas para indicar la necesidad de asegurar la no modificación del contenido de los correos enviados por sus empleados.

11.- Otro de los principales problemas del envío de correo electrónico es asegurar que el correo enviado ha llegado al destinatario.

La aplicación Lotus Notes implementa una opción de acuse de recibo para que cuando el receptor del mensaje lo lea, nos llegue de forma automática un acuse de recibo en que se notifica que el destinatario del mensaje lo ha recibido y lo ha leído.

Esta opción tampoco es obligatoria, pero para las organizaciones puede ser muy interesante su utilización, ya que de esta forma el remitente de un mensaje crítico puede estar totalmente seguro, que dicho mensaje no sólo se entregó de forma correcta sino que además su destinatario lo ha leído.

La organización debería implementar las políticas necesarias para asegurar la recepción de los correos electrónicos enviados por los empleados de la organización e indicar la importancia para la organización de poder asegurar que los correos electrónicos enviados se entregan de forma correcta.

12.- Uno de los mayores peligros de la recepción de correos electrónicos son los ficheros adjuntos y las imágenes incrustadas sobre el cuerpo del mensaje, debido a que no es posible asegurar la autoría de todos los correos recibidos hay un alto índice de probabilidad que el fichero adjunto o la imagen incrustada sea un archivo dañino o virus.

La aplicación Lotus Notes dispone de una opción que permite no descargar de forma automática ni las imágenes incrustadas en el texto ni los ficheros adjuntos al correo electrónico, de esta forma se pueden evitar posibles ataques a los sistemas informáticos de la organización a través de correos electrónicos, aunque cabe destacar que con la implementación de esta opción de la aplicación Lotus Notes no se asegura que algún empleado por descuido o por estar resentido con la organización ejecute un fichero peligroso, adjunto a un correo electrónico, potencialmente dañino para la organización.

La organización debería implementar las políticas internas necesarias que evitasen este problema e indicasen la importancia para la organización que todos los empleados de la organización la lleven a cabo.

13.- Aunque no suele ser muy habitual algunas organizaciones disponen de políticas internas en las que se indica cómo deben tratarse los correos electrónicos recibidos, es decir, tienen políticas internas en las que se indica si cierto tipo de correos se deben o pueden descargar de formar automática a un equipo local, o si deben ser introducidos de forma inmediata en alguna carpeta de correo electrónico en concreto.

Para verificar que este tipo de políticas se cumplen correctamente se debe comprobar qué tipo de filtros de correo están implementados en la aplicación Lotus Notes y si están implementados en la forma indicada en las políticas, es decir, si la política dice que un correo electrónico se debe mover a una carpeta específica pero debe quedar copia en la bandeja de entrada, se debe comprobar que la aplicación Lotus Notes lo mueve a la carpeta específica y que no lo elimina de la bandeja de entrada, o al revés si la política indica que se debe borrar de la bandeja de entrada se debe comprobar que el correo es eliminado de la bandeja de entrada.

14.- También en algunas organizaciones existen políticas internas que disponen la forma en la que se deben contestar ciertos correos, ya sean de ventas, compras, peticiones de servicio, reclamaciones,…

Para verificar que este tipo de políticas se cumplen en la forma establecida en las políticas internas se deberían comprobar todas las plantillas existentes en la aplicación Lotus Notes y comprobar que cumplen con lo establecido en las distintas políticas internas, también se

debería revisar una nuestra lo más aleatoria y heterogénea posible de los correos enviados mediante la utilización de las plantillas para verificar que se utilizan en la forma establecida por la política interna de la organización.

Pero esto puede ser muy costoso en tiempo ya que si el volumen de empleados de la organización es elevado habría que revisar muchísimos correos electrónicos, por lo que lo más eficiente es simplemente incluir una pregunta en los cuestionarios al respecto.

15.- Aunque en la organización no exista ninguna normativa interna concreta al respecto, todo el software instalado en los equipos de la organización debe poseer su correspondiente licencia en regla y que esté correctamente actualizado, y la aplicación Lotus Notes y el sistema operativo de los equipos informáticos en lo que se encuentre instalada no deben ser una excepción a esta norma.

De esta forma se evitará que por tener productos de software desactualizados o anticuados los equipos estén sometidos a vulnerabilidades que pueden estar solventadas en versiones posteriores o parches.

16.- En todas las organizaciones debe de existir una política de gestión de copias de seguridad de la información que maneja la organización, en algunas organizaciones será de la gran mayoría de datos de los que dispone y en otras organizaciones sólo de los datos más importantes, en nuestro caso deberemos comprobar si existe alguna política de copias de seguridad respectiva al correo electrónico y si se aplican sobre la aplicación Lotus Notes, en cuyo caso deberemos comprobar que sólo se

copian los archivos indicados en la política de copias de seguridad y que las copias realizadas se protegen en la forma indicada en la política interna de la organización.

Ya que si no se cifran los datos almacenados en la aplicación Lotus Notes (correos, libreta de direcciones,…) si se realizan copias de seguridad cualquiera que tenga acceso a las copias de seguridad, ya sea una persona que tenga acceso autorizado a las copias como una que no lo tenga, podrá tener acceso a los datos almacenados en la aplicación Lotus Notes.

17.- Es conveniente que las contraseñas del personal de la organización para el acceso a la aplicación Lotus Notes y el acceso a los diferentes equipos informáticos de la organización sean diferentes, para evitar que si una de las dos contraseñas se ve comprometida, se tenga acceso tanto a la aplicación Lotus Notes como a los diferentes equipos informáticos.

Es conveniente destacar que la aplicación Lotus Notes permite sincronizar las contraseñas de inicio de sesión de los equipos Windows con la de inicio de sesión en la aplicación Lotus Notes, por lo que se deberá comprobar si la opción de sincronización de contraseña se encuentra activa en la configuración de Lotus Notes.

De esta forma no se puede estar completamente seguro que los empleados no utilicen una única contraseña para acceder a los diferentes sistemas informáticos y aplicaciones; pero al menos se evita que se inicie la sesión de la aplicación Lotus Notes de forma automática al iniciar sesión en los sistemas informáticos de la organización.

Ahora que hemos enumerado los distintos riesgos a los que puede estar sometida la aplicación Lotus Notes procederemos a asignarles prioridades

relativas a los distintos riesgos evaluados, aunque cabe destacar que estas prioridades sólo son válidas para el tema que nos ocupa, ya que las prioridades de las distintas organizaciones no tienen ninguna razón por la que ser iguales, a excepción, claro está, que se encargue una auditoría de la aplicación Lotus Notes desde el punto de vista de la seguridad, en cuyo caso las prioridades deberían ser muy similares a las expuestas a continuación.

Los riesgos que deben tener una mayor prioridad, serán aquellos que sean más críticos respecto al tema que nos ocupa, es decir, los relativos a la seguridad en la aplicación Lotus Notes como aplicación de correo electrónico y los que deben tener menor prioridad son los referentes a normativa interna no aplicable al ámbito de nuestra auditoría.

Podemos agrupar los riesgos anteriores en 4 grupos en función de su prioridad en relación al ámbito del presente proyecto final de carrera, es decir, en relación a la seguridad de la información contenida en la aplicación Lotus Notes, vista como aplicación de correo electrónico.

El grupo 1 que es el de mayor prioridad incluye los riesgos 2, 4, 7, 15 y 17

El grupo 2 incluye los riesgos 1, 3, 5, 6 y 8.

El grupo 3 incluye los riesgos 9, 10, 11 y 12.

Y el grupo 4 que es el de menor prioridad incluye los riesgos 13, 14 y 16.

Podemos decir que los riesgos del grupo 1 son aquellos que afectan de forma más directa a la integridad de la información contenida en la aplicación Lotus Notes, ya que si alguno de estos riesgos se materializa la obtención de la información alojada en la aplicación Lotus Notes es inmediata, por este motivo hemos decidido catalogar estos riesgos como los de mayor prioridad.

Los riesgos pertenecientes al grupo 2 son aquellos que afectan a la integridad de la información contenida en la aplicación Lotus Notes, pero de una forma más indirecta, ya que cualquier persona que intentase obtener los datos a través de alguno de los riesgos de este grupo, debería realizar alguna acción adicional para obtener la información que se encuentra en la aplicación Lotus Notes, por este motivo los riesgos de este grupo son los segundos en prioridad.

Los riesgos pertenecientes al grupo 3 son aquellos que afectan a la integridad de los mensajes, del destinatario y/o del remitente, es decir, los que no afectan a la información almacenada en la aplicación Lotus Notes, pero sí afectan a la información que se envía o que se recibe desde la aplicación Lotus Notes.

Los riesgos pertenecientes al grupo 4 son todos los demás riesgos que no quedan recogidos en los tres primeros grupos, es decir, son los relacionados con posibles políticas de la organización pero que no afectan a la seguridad o lo hacen de forma muy indirecta a la aplicación Lotus Notes.

6.3 COMPROBACIÓN DE LOS RIESGOS.

A lo largo de este punto mostraremos cuál es la configuración correcta de los diferentes parámetros de la aplicación Lotus Notes para evitar o minimizar los riesgos relacionados con la aplicación Lotus Notes evaluados en el punto anterior.

En primer lugar mostraremos la configuración correcta de la aplicación Lotus Notes para que pida usuario y contraseña cada vez que se inicia sesión en la aplicación. Para poder verificar si esta opción es usada por los empleados se podría ir ordenador por ordenador iniciando sesión en todos ellos y arrancando la aplicación Lotus Notes y comprobar si solicita usuario y contraseña; pero este proceso además de ser muy lento no asegura que la opción este permitida o no. Para verificar si durante la instalación de la aplicación Lotus Notes se instaló la opción de sincronización de contraseña con Windows, también conocida como función *single logon para el cliente*, debemos comprobar dentro de la seguridad de usuario si dicha opción es seleccionable, los pasos a seguir se muestran en las siguientes imágenes.

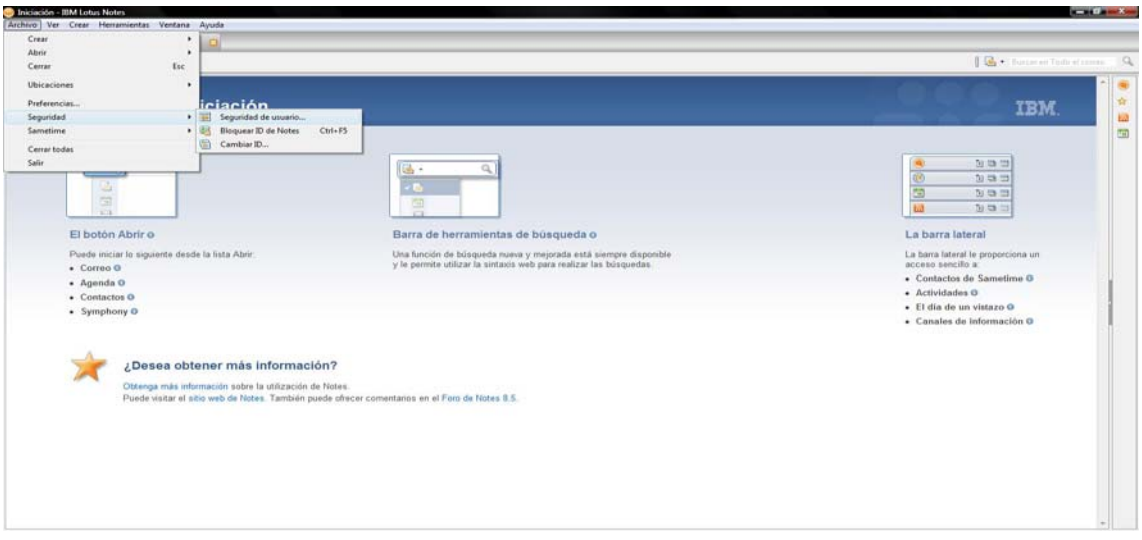

Figura 6.1: Acceso a las opciones de seguridad del usuario.

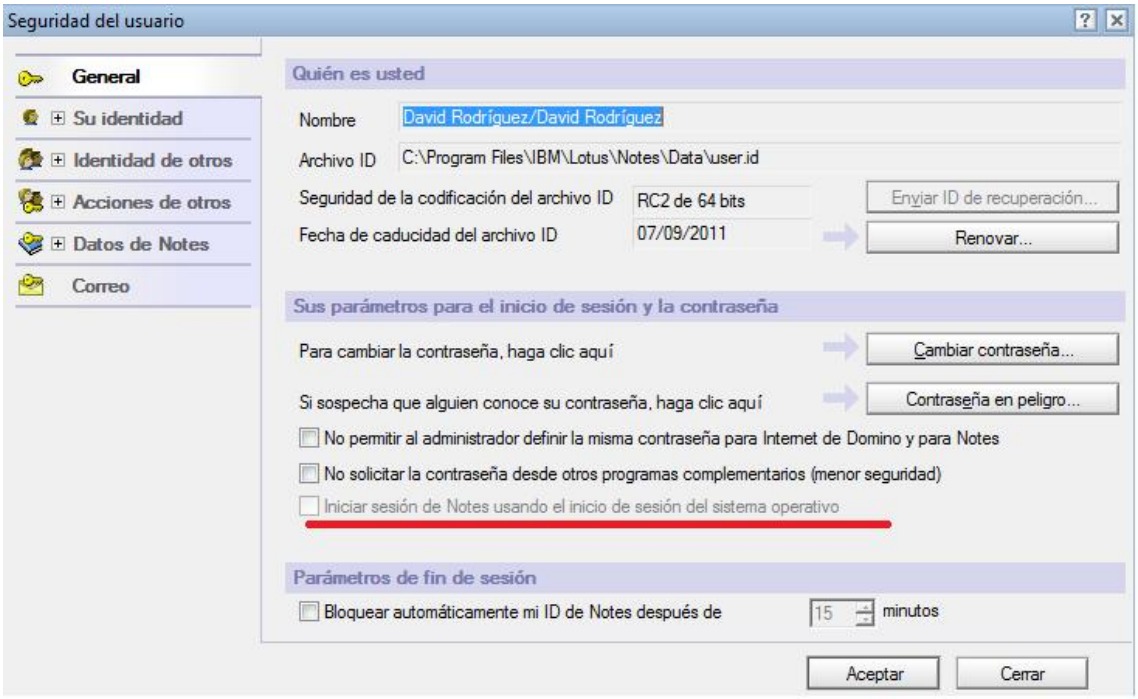

Figura 6.2: Opción de sincronización de contraseñas.

Como podemos comprobar en la imagen 6.2., la función *single logon* en este caso no se encuentra instalada, ya que no es posible seleccionarla para que una vez iniciada la sesión en los equipos Windows se inicie también sesión de forma automática en la aplicación Lotus Notes.

A continuación indicaremos cuál debe ser la configuración correcta de la aplicación Lotus Notes para que se bloquee de forma automática tras un periodo de inactividad determinado, indicado por cada usuario. Para activar el bloqueo automático debemos acceder a la seguridad del usuario, tal y como se indica en la figura 6.1., que aparece en la página anterior, y en la página que aparece a continuación debemos hacer click sobre la opción *Bloquear automáticamente ID de Notes después de* e indicamos el tiempo que deseamos que trascurra hasta que la aplicación Lotus Notes se bloquee de forma automática por inactividad, debemos recordar que si la organización dispone de

alguna política sobre bloqueo de sesiones debemos comprobar que se cumple, es decir, el tiempo del bloqueo automático debe coincidir con el indicado en la política interna descrita por la organización.

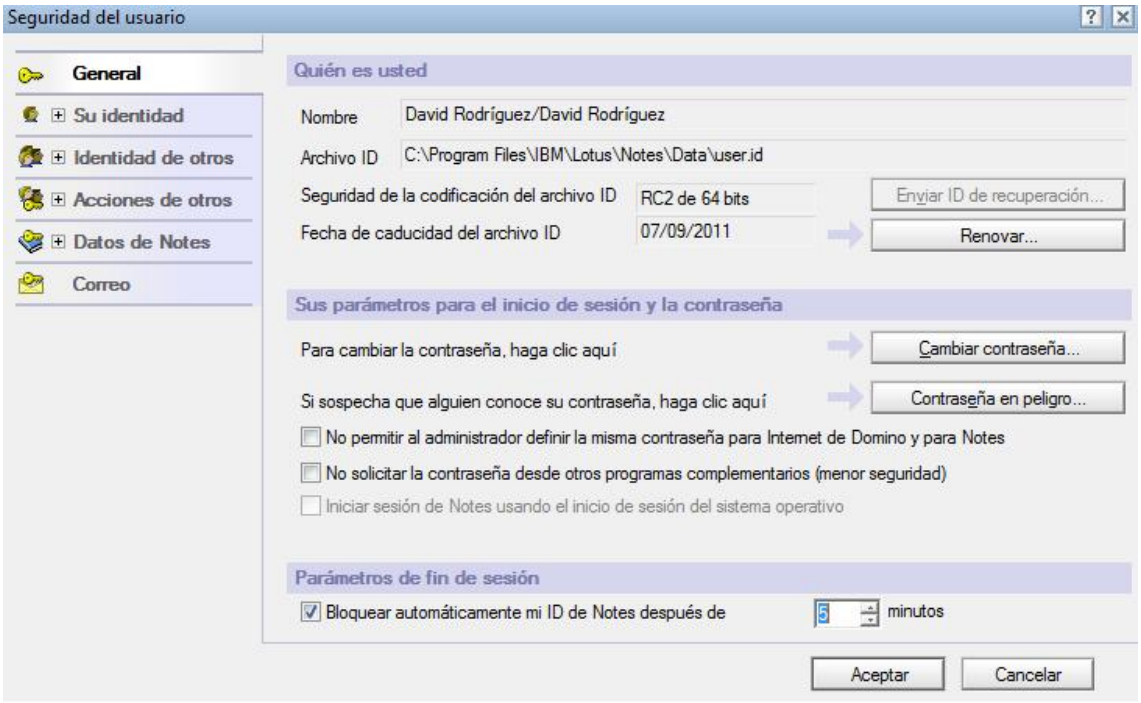

Figura 6.3: Opción de bloqueo automático.

Ahora indicaremos qué pasos debemos seguir para comprobar que el contenido almacenado en la aplicación Lotus Notes no es accesible desde fuera de la misma, y que además sólo es accesible a través de la aplicación Lotus Notes por su dueño, o en su defecto, por las personas autorizadas por el propietario. En primer lugar accedemos a la seguridad del usuario, tal y como se indica en la Figura 6.1., una vez dentro de las opciones de seguridad del usuario comprobamos si se realiza el cifrado de las base de datos de la aplicación Lotus Notes, tal y como se muestra en la figura 6.4.

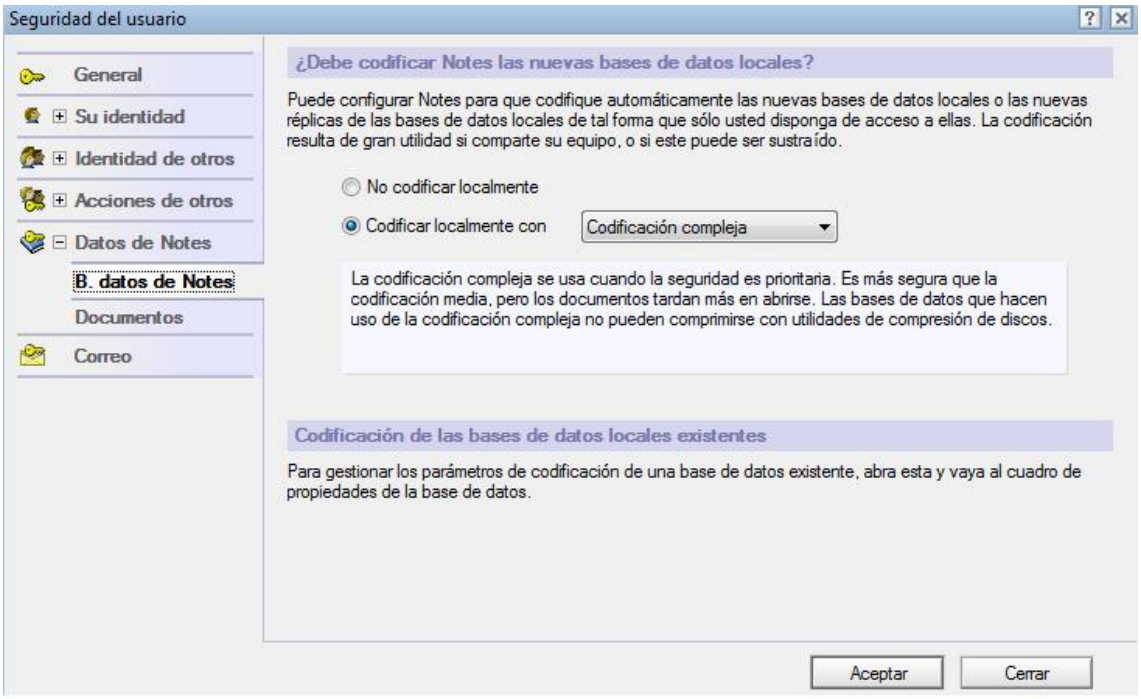

Figura 6.4: Cifrado de los componentes de Lotus Notes.

Es conveniente destacar que la aplicación Lotus Notes dispone de tres niveles de cifrado, cifrado sencillo, cifrado medio y cifrado complejo. El cifrado sencillo se limita únicamente a restringir el acceso a nivel de usuarios, el cifrado medio es más seguro que el sencillo y otorga una velocidad de acceso a las bases de datos óptima, mientras que el cifrado complejo es el más seguro con diferencia pero ralentiza el acceso a las bases de datos, por lo que sólo se recomienda su uso para aquellos contenidos de máxima prioridad para la organización.

Seguidamente indicaremos los pasos que debemos seguir para comprobar si se realiza el cifrado de la copia de todos los correos enviados, ya que si no se cifran, cualquier persona que tuviese acceso al equipo informático y a la aplicación Lotus Notes podría tener acceso a la información contenida en los correos enviados, es decir, tendría acceso a las direcciones de correo de los distintos destinatarios de los correos electrónicos y al contenido de los mismos.

Accedemos a la seguridad del usuario, tal y como se muestra en le figura 6.1 y en la parte de correo comprobamos si la opción de *codificar la copia de los correos que se envíe* está marcada tal y como se muestra en la Figura 6.5.

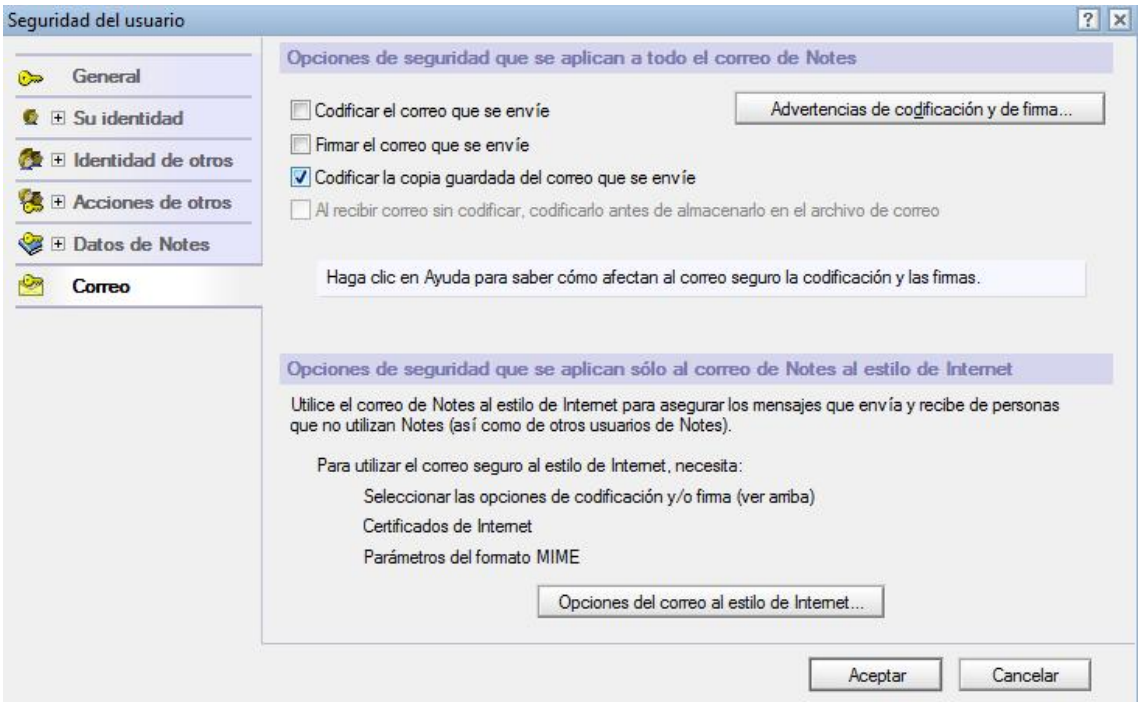

Figura 6.5: Cifrado copia de correos enviados.

Nos queda comprobar que sólo los usuarios que deben tener acceso a los datos almacenados en la aplicación Lotus Notes lo tienen, y que el resto de usuarios de la aplicación sólo puedan acceder a los contenidos que aparezcan reflejados en la política interna de la empresa, en el caso de que exista alguna, de no ser así ningún usuario de la aplicación Lotus Notes debería tener acceso, total o parcialmente, al correo electrónico de otro usuario de la aplicación Lotus Notes. Primero se debe acceder al control de acceso del correo electrónico, por lo que deberemos entrar en la pestaña del correo electrónico y seleccionar control de acceso, tal y como se muestra en la figura 6.6.

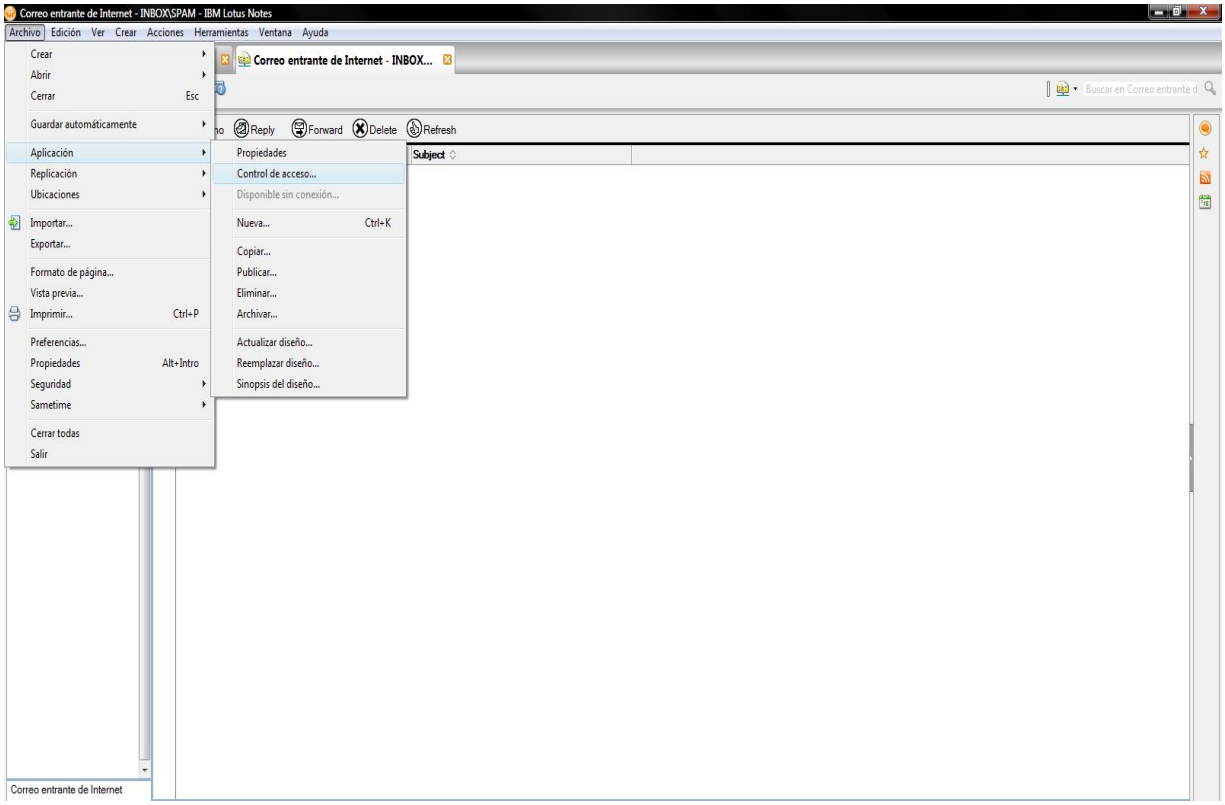

Figura 6.6: Control de acceso al correo electrónico.

Dentro de las opciones de control de acceso debemos comprobar que los permisos de cada usuario, grupo o servidor, son los especificados en las políticas de seguridad de la organización, tal y como se muestra en la figura 6.7.

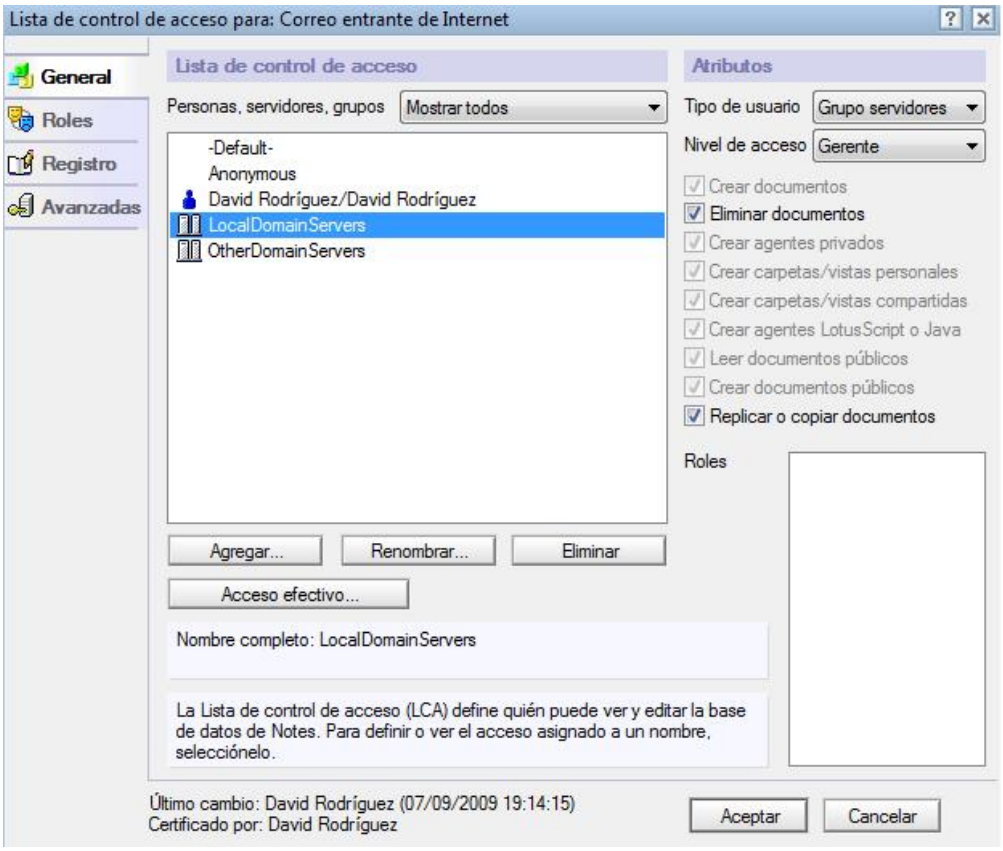

Figura 6.7: Listado del control de acceso al correo electrónico.

Como se puede comprobar en la figura anterior existen diferentes tipos de usuario y de nivel de acceso, en función de cada nivel de acceso, los usuarios o los grupos de usuarios podrán realizar más o menos acciones sobre los correos electrónicos, como se puede apreciar en la figura anterior, en función del nivel de acceso de cada usuario se pueden añadir o eliminar acciones. Por lo tanto, se deben revisar las políticas internas de la organización para verificar que se cumplen o en caso contrario indicar que modificaciones sobre la configuración de la aplicación Lotus Notes se deben realizar para que la normativa interna de la organización se cumpla.

Una vez verificado qué usuarios tienen acceso al correo electrónico a través de la aplicación Lotus Notes y qué acciones pueden realizar sobre él mismo, debemos comprobar que aplicaciones pueden tener acceso a los diferentes

componentes de la aplicación Lotus Notes, en función de qué persona sea la creadora de la aplicación, es decir, en función de qué persona es la que firma la aplicación. Se debe comprobar en las distintas políticas internas de la empresa qué personas o grupos pueden realizar qué acciones sobre la aplicación Lotus Notes, podemos verificarlo a través de la seguridad de usuario, como se muestra en la figura 6.1., una vez dentro de las opciones de seguridad, podemos comprobar y modificar qué aplicaciones tienen acceso a qué componentes de la aplicación Lotus Notes dentro de *acciones de otros*, tal y como se muestra en la siguiente figura.

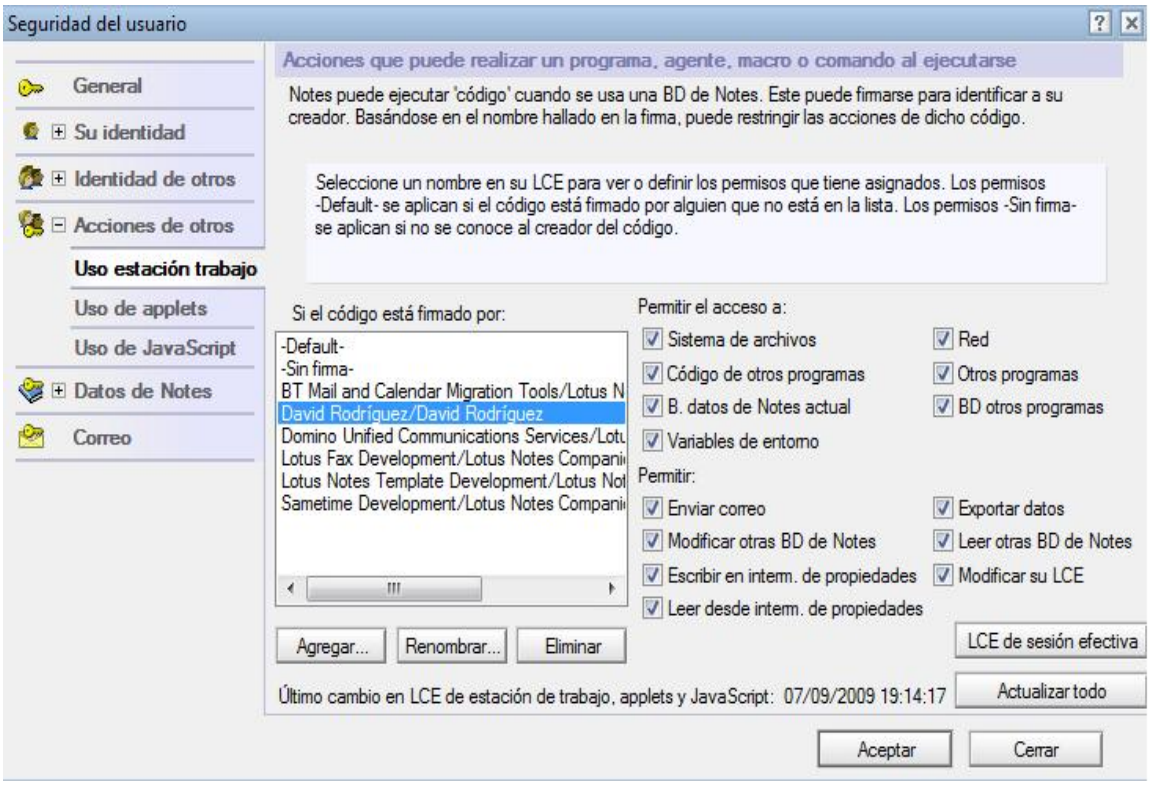

Figura 6.8: Opciones de acceso de aplicaciones a Lotus Notes

Como comentamos en al punto 6.2 es muy recomendable que las contraseñas de acceso se modifiquen periódicamente, para evitar que pueda ser capturada o adivinada por algún atacante a la aplicación Lotus Notes o de los

sistemas informáticos de la organización. En caso de existir alguna política interna de la organización que especifique los plazos de validez de las contraseñas debemos intentar comprobar que dichos plazos se cumplen, pero desgraciadamente si la aplicación Lotus Notes no está conectada a ningún servidor de Lotus Domino, como es nuestro caso, no podemos realizar las comprobaciones reales; pero lo que sí podemos mostrar es dónde se puede cambiar la contraseña y dónde se podría verificar cuando fue la última vez que se realizo el cambio de contraseña. Para cambiar la contraseña de acceso a la aplicación Lotus Notes, se debe acceder a la seguridad del usuario, tal y como se muestra en la figura 6.1 y dentro de las opciones generales pinchar sobre *cambiar contraseña,* tal y como se refleja en la figura 6.3.

En la nueva pantalla se debe introducir la nueva contraseña y el tipo de codificación de la misma, tal y como se refleja en la siguiente figura:

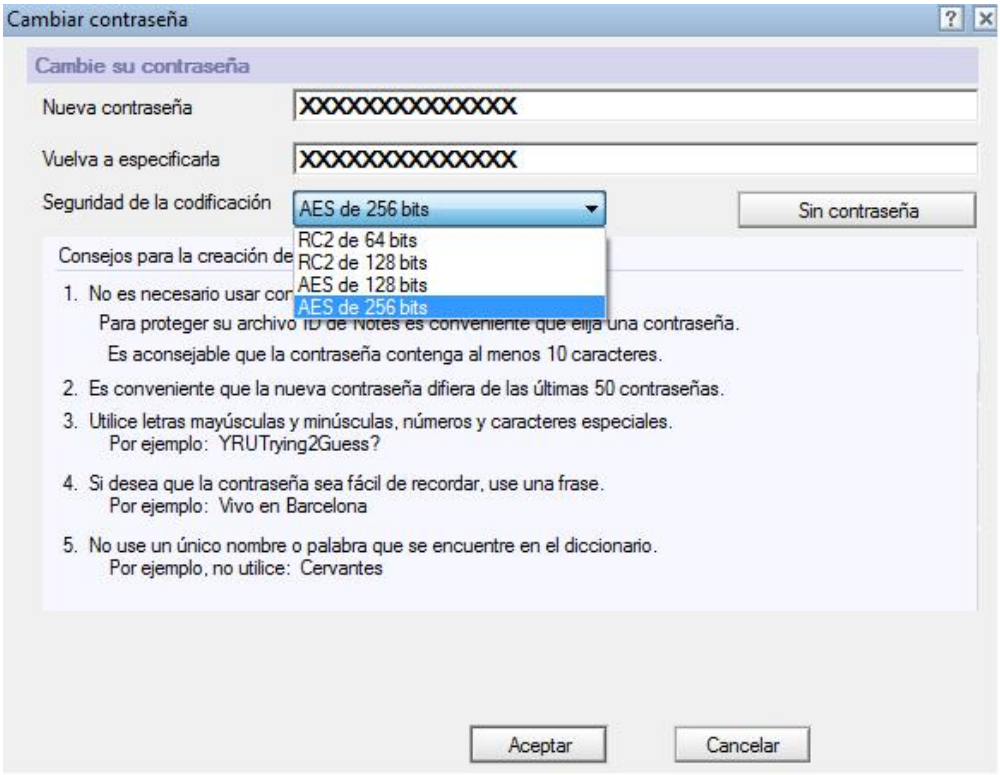

Figura 6.9: Nueva contraseña de acceso a Lotus Notes.

Para comprobar cuándo fue la última vez que un usuario cambio su contraseña de acceso a la aplicación Lotus Notes, se deben seguir los mismos pasos que para cambiar la contraseña, pero en lugar de pinchar sobre *cambiar contraseña* se debe pinchar sobre *contraseña en peligro*¸ tal y como aparece reflejado en la figura 6.3 y en la nueva pantalla que aparece se debe pinchar sobre *comprobar contraseña,* tal y como se refleja en la siguiente figura.

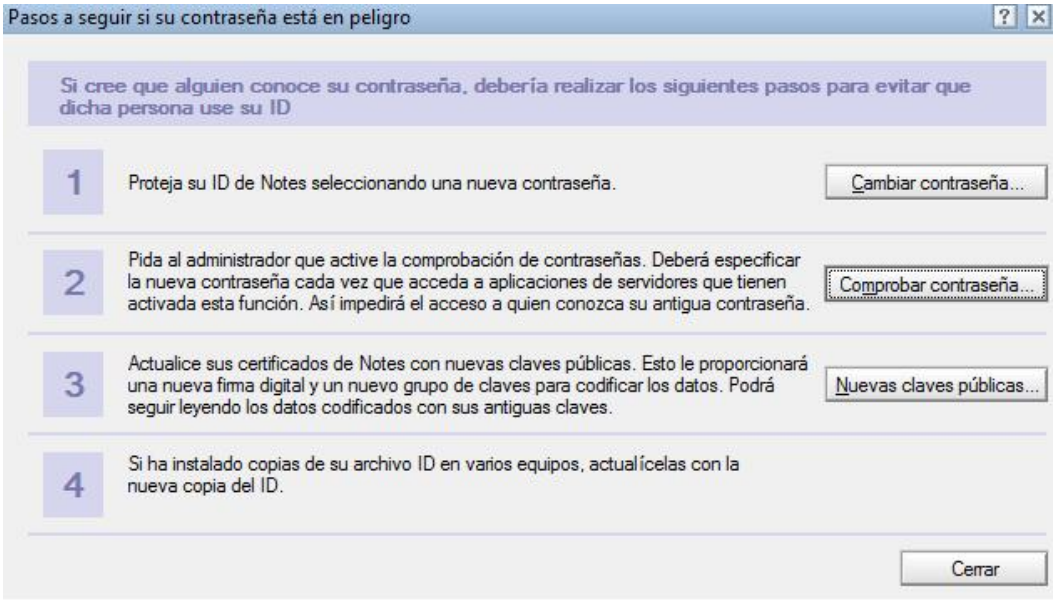

Figura 6.10: Comprobación últimos cambios de contraseña.

Si la aplicación Lotus Notes estuviese conectada a un servidor de Lotus Domino, se podría comprobar en la página que aparece tras pinchar en *comprobar contraseñas*, cuándo fue la última vez que el usuario cambio la contraseña; además el administrador de Lotus Domino, puede obligar a todos los usuarios de la aplicación Lotus Notes a cambiar la contraseña tras un determinado periodo de tiempo, que en el caso que la organización dispusiera de alguna política de cambio de contraseñas, debería ser el indicado en las políticas de la organización.

La aplicación Lotus Notes al realizar operaciones de envío de mensajes o de actualización sobre sus bases de datos, primero realiza una copia local de los mismos en el directorio temporal de la aplicación, este directorio dependerá de la ruta de instalación de la aplicación, en nuestro caso será *C:/Archivos de programa/Ibm/Lotus Notes/Data/workspace/logs*, los archivos temporales de la aplicación Lotus Notes suelen tener extensiones nsp o rtf; pero contra lo que cupiese esperar la aplicación Lotus Notes si produce algún fallo durante la ejecución para la que fue creada el fichero temporal, el fichero temporal no se elimina, sino que se queda en el directorio temporal como fichero corrupto y aunque en teoría su contenido no es accesible ni reproducible, ya que la propia aplicación Lotus Notes no es capaz de utilizarlo en el caso de que se reintente la operación que fallo, sino que vuelve a generar un nuevo fichero temporal para realizar el envío o la actualización de la base de datos. Por lo tanto, los ficheros temporales generados por la aplicación Lotus Notes se deben eliminar de forma manual del disco duro de los equipos, ya que aunque en teoría su contenido no es reproducible ni accesible es muy recomendable eliminarlos por si en un futuro su contenido sí es accesible desde la aplicación Lotus Notes o desde cualquier otra aplicación.

Para comprobar que los correos enviados desde la aplicación Lotus Notes se envían con autenticación de remitente, para que el receptor del correo electrónico pueda tener la certeza que el remitente que aparece en la cabecera del correo es el verdadero remitente del mensaje. Obviamente el primer paso será comprobar que exista una firma digital en la aplicación Lotus Notes, no explicaremos como se puede obtener una firma digital ya que no es materia del actual proyecto fin de carrera ni como se puede introducir una firma dentro de

la aplicación Lotus Notes, es conveniente destacar que si un mismo usuario puede utilizar distintos equipos informáticos para acceder al correo electrónico a través de la aplicación Lotus Notes deberá tener su clave digital en todos los equipos informáticos que utilice para acceder al correo electrónico a través de la aplicación Lotus Notes. Para comprobar tanto la existencia en los equipos de una firma electrónica como que los correos electrónicos enviados son firmados debemos acceder a la seguridad de usuario tal y como se muestra en la figura 6.1., para el caso de comprobar la existencia de certificados debemos entrar en *Su identidad* y dentro de este menú en *Sus certificados* tal y como se muestra en la Figura 6.11.

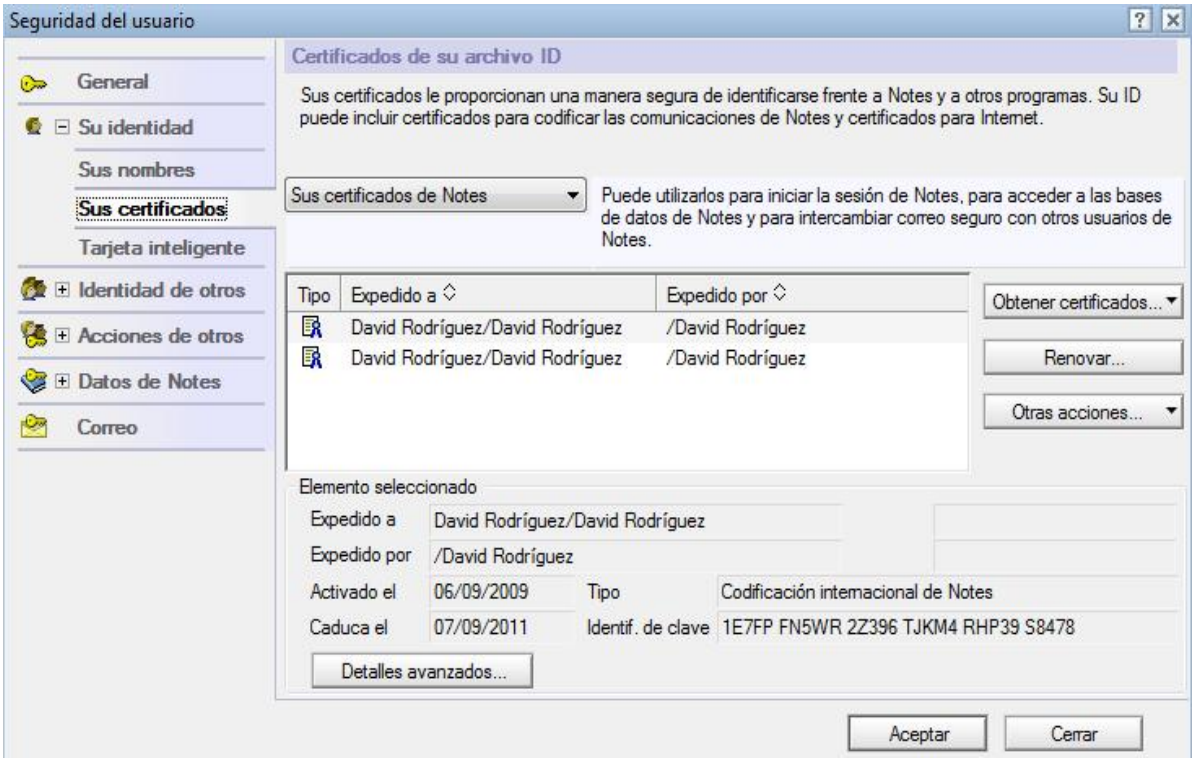

Figura 6.11: Comprobación de existencia de firmas digitales.

La aplicación Lotus Notes admite tanto los certificados generados por la propia aplicación como cualquier otro certificado digital expedido por cualquier entidad certificadora.

Para comprobar que los correos electrónicos enviados a través de la aplicación Lotus Notes se envían de forma segura, en primer lugar podemos comprobar si los correos electrónicos son cifrados al ser enviados, esta es una opción de la aplicación Lotus Notes muy útil que permite realizar envíos de forma segura basándose únicamente en certificados digitales, para comprobar si esta opción está activa debemos acceder a la seguridad de usuario tal y como se refleja en la figura 6.1., dentro de las opciones de usuario nos vamos a las de correo y comprobamos si la opción *codificar el correo que se envíe* está marcada, tal y como se muestra en la figura 6.12.

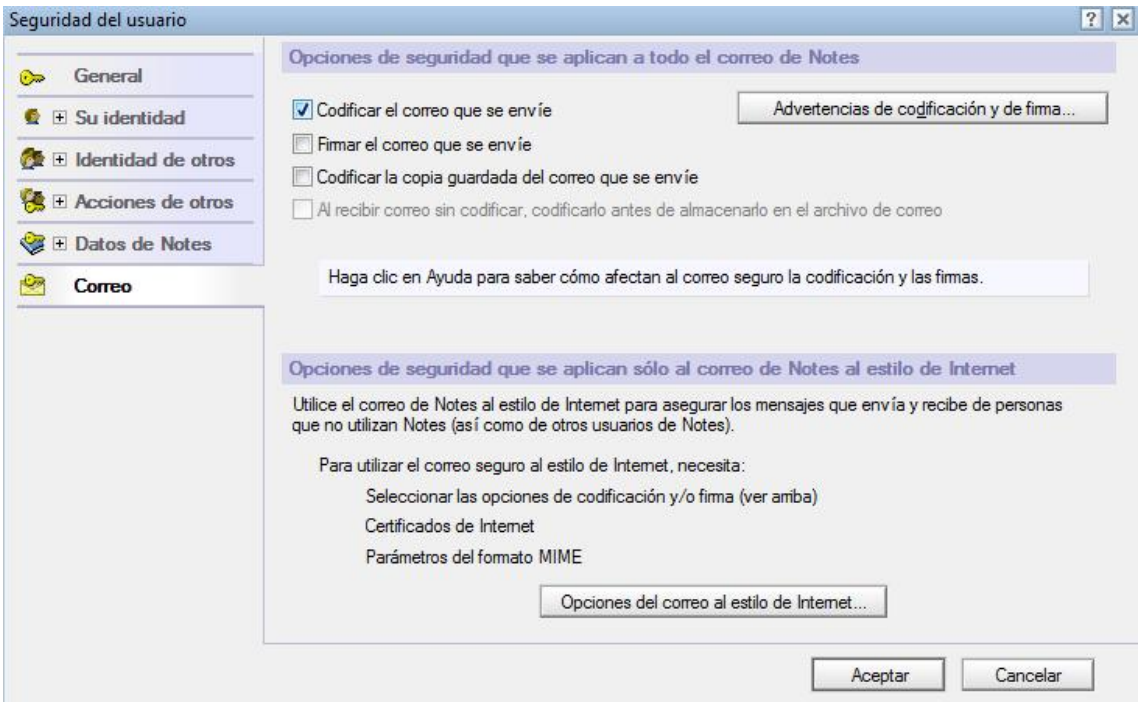

Figura 6.12: Comprobación de cifrado del correo enviado.

Otra forma de enviar correos seguros es utilizando el protocolo SSL en el envío de los mensajes, por lo que se debe comprobar que la configuración de los servidores de correo entrante y saliente permiten la posibilidad de utilizar dicho protocolo. Primero se debe acceder a las preferencias generales de la aplicación Lotus Notes, tal y como se muestra en la siguiente figura.

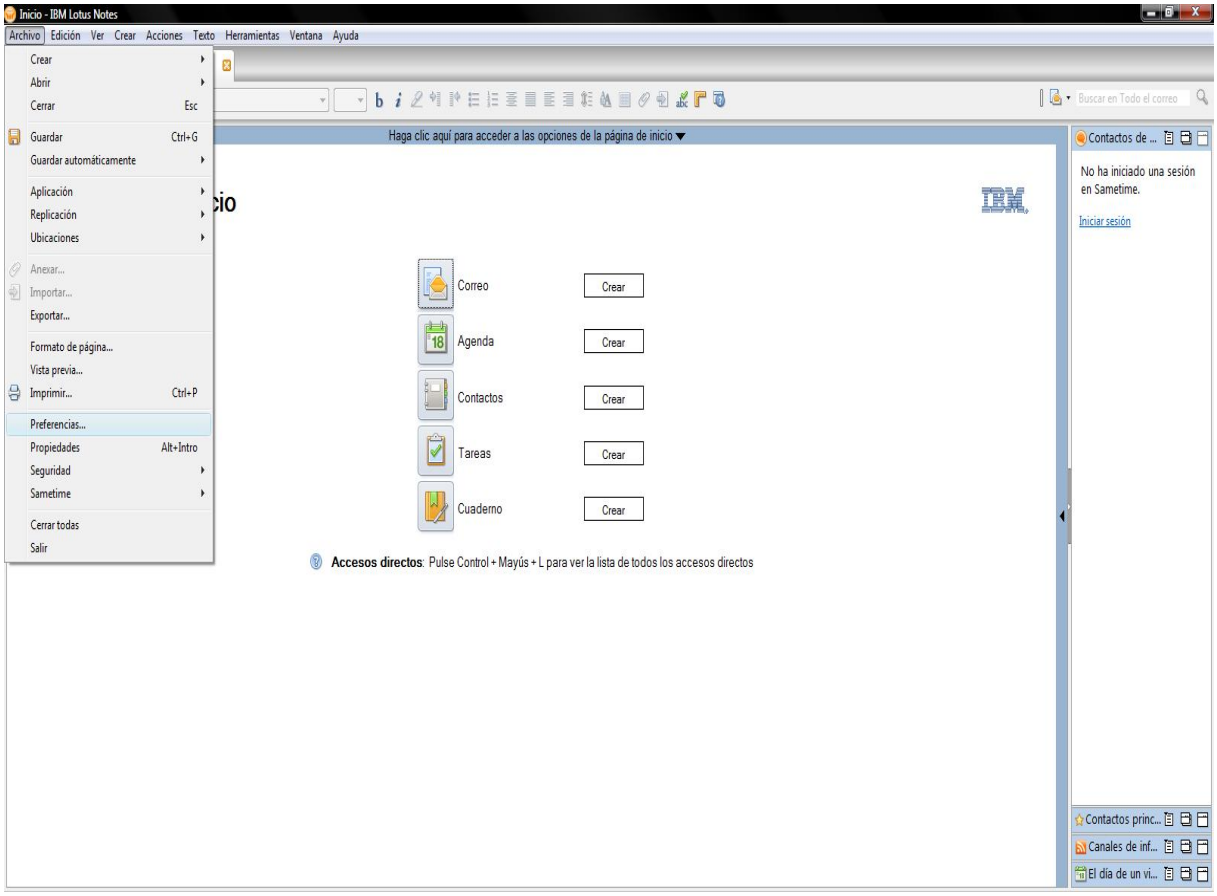

Figura 6.13: Acceso a las preferencias de la aplicación Lotus Notes

Dentro de las preferencias comprobamos en *cuentas* la configuración de los servidores de correo electrónico entrante y saliente, tal y como se muestra en siguiente figura.

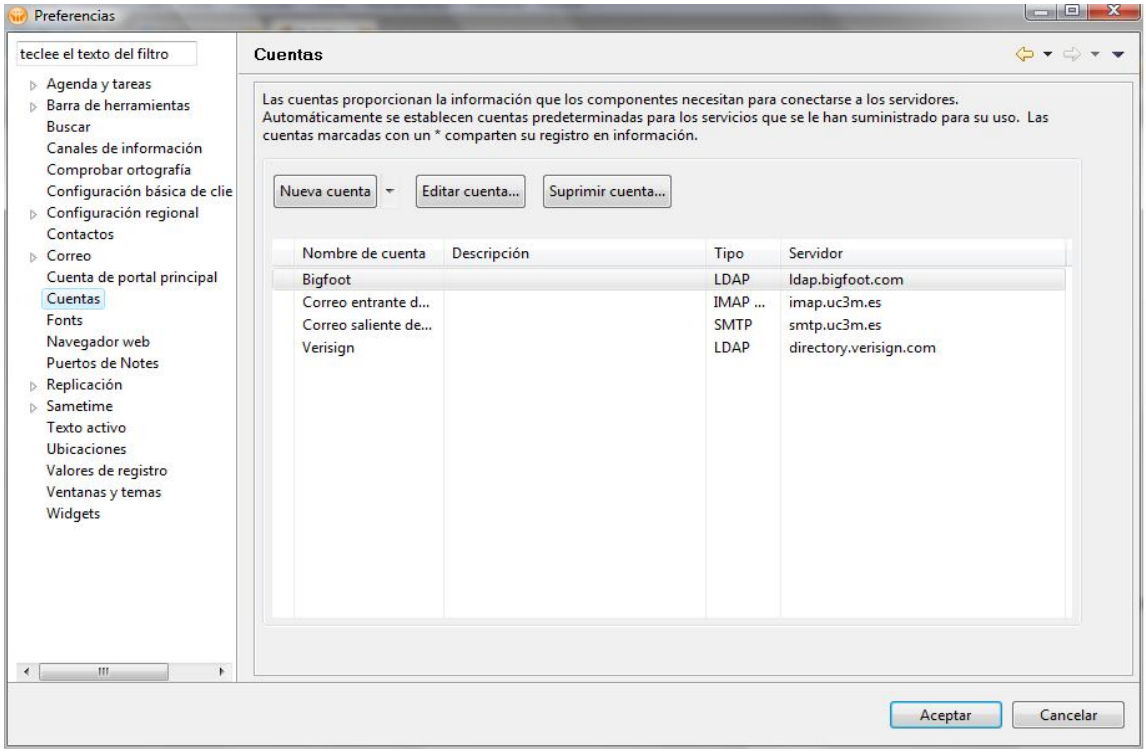

Figura 6.14: Acceso a la configuración de los servidores de correo.

Una vez dentro de Cuentas debemos comprobar la configuración de los servidores de correo electrónico entrante y saliente, para ello nos fijamos en la columna tipo y si el envío SSL estuviese habilitado aparecería así reflejado, y en lugar de aparecer SMTP e IMAP aparecería SMTP (SSL habilitado) y IMAP (SSL habilitado), respectivamente.

Para comprobar si los usuarios de la aplicación Lotus Notes tienen activada la descarga automática de imágenes incrustadas en el texto del mensaje, lo que como hemos comentado anteriormente supone una alta probabilidad de infección por virus informático, se debe acceder a las preferencias de la aplicación tal y como se muestra en la figura 6.13 y dentro de las preferencias se debe acceder a las de correo y comprobar que la opción *no mostrar*

imágenes remotas sin mi permiso está activada, tal y como se muestra en la siguiente figura.

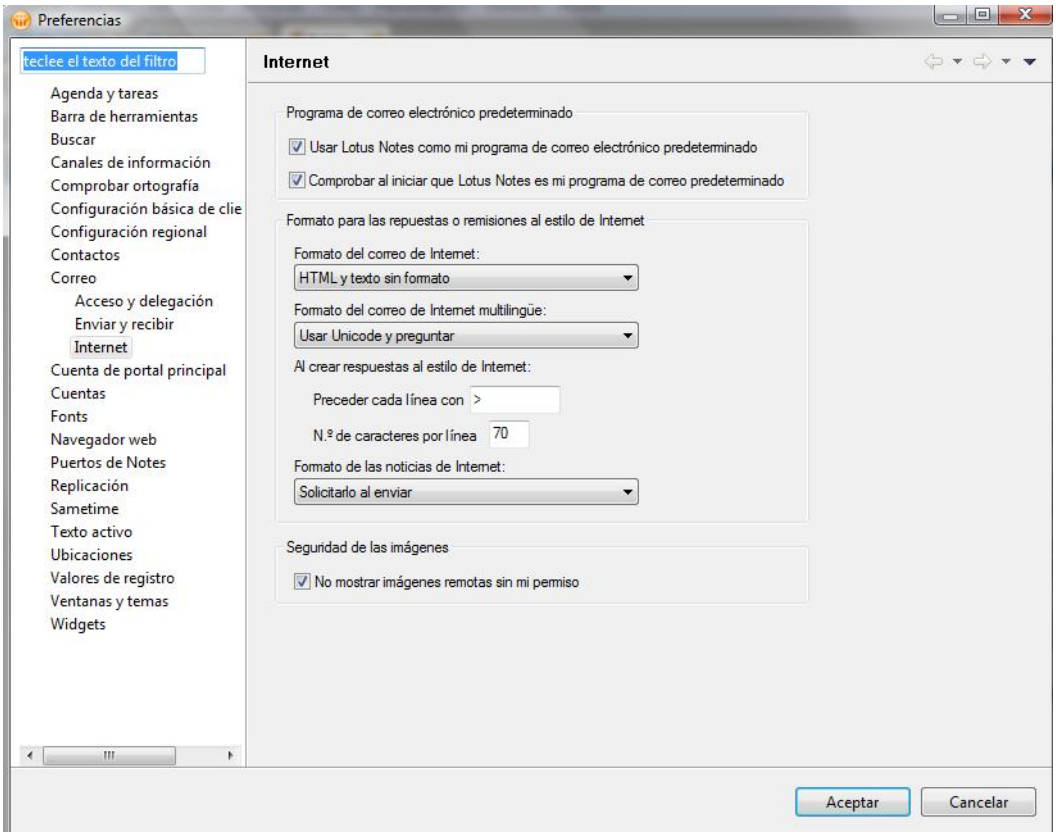

Figura 6.15: Comprobación de no descarga de imágenes incrustadas en los mensajes.

Para comprobar que la aplicación Lotus Notes dispone de una licencia completa o si por el contrario se trata de cualquier otro tipo de licencia, deberemos mirar dentro del directorio de instalación de la aplicación, que por defecto se suele instalar en *C:\Archivos de programa\IBM\Lotus\Notes* y dentro de este directorio debe haber una carpeta con el nombre *license* que debe contener varios archivos con extensión rtf, podemos comprobar el tipo de licencia directamente desde el archivo *nob_ibm_license.rtf* o sobre cualquiera de los archivos *LA_xx.rtf*, las x del nombre de estos ficheros hacen referencia al idioma, es decir, en el archivo *LA_es.rtf* estará la descripción de la licencia en

castellano y en el archivo *LA_it.rtf* estará la descripción de la licencia en italiano. Como comentamos en el punto 6.2 es de vital importancia que las organizaciones tengan debidamente licenciada la aplicación Lotus Notes para poder disfrutar de todas sus funcionalidades.

El resto de riesgos que aparecen reflejados en el punto 6.2 y que no aparecen reflejados a lo largo del punto 6.3., o bien no hacen referencia de forma directa a la aplicación Lotus Notes o no es posible realizar con el suficiente rigor su comprobación, como son el caso del uso de plantillas para enviar y contestar correos o el archivado de los mensajes enviados y recibidos, ya que no es posible comprobar todos los correos enviados y recibidos de todos los usuarios.

6.4 REALIZACIÓN DE LOS CUESTIONARIOS.

Antes de realizar el cuestionario debemos tener en cuenta los diferentes perfiles de los entrevistados y si en función de esos perfiles será necesario crear distintos tipos de cuestionarios o crear preguntas específicas para algunos perfiles y que el resto de preguntas sean comunes para todos los perfiles.

En nuestro caso hemos creído más conveniente realizar un único tipo de cuestionario con una serie de preguntas comunes para los distintos perfiles de entrevistados, y añadir algunas preguntas específicas a cada tipo de perfil; pero la estructura del cuestionario será común para todos ellos.

A continuación enumeraremos los diferentes tipos de perfiles que hemos decidido diferenciar y qué motivo nos ha movido a realizar dicha diferenciación.

En primer lugar hemos diferenciado entre los administradores y los usuarios normales de la aplicación Lotus Notes, dentro del grupo de usuarios normales hemos diferenciado entre usuarios avanzados o expertos y usuarios principiantes. Podemos definir a usuarios expertos o avanzados como aquellas empleados de la organización que llevan trabajando en la organización durante varios años y que debido al tipo de trabajo que desempeñan deben utilizar a diario la aplicación Lotus Notes, como por ejemplo el personal de secretaría, el compras y ventas, … Por el contrario los usuarios principiantes son aquellos que llevan poco tiempo en la organización o aquellos que aún llevando bastantes años en la organización, debido al tipo de trabajo que desempeñan usan con poca frecuencia la aplicación Lotus Notes como pueden ser los programadores, el personal de mantenimiento, …

Creemos que haciendo la diferenciación anterior quedarían cubiertos los diferentes tipos de usuarios con acceso a la aplicación Lotus Notes, y por lo tanto podríamos crear una visión bastante completa del modo en el qué se accede y de la configuración de la aplicación Lotus Notes y las medidas de seguridad tomadas para tratar de asegurar su correcto funcionamiento y limitar el uso de la aplicación sólo a las personas de la organización autorizadas a utilizarla.

Ahora procederemos a enumerar las diferentes preguntas que debemos hacer a los entrevistados para poder realizar de forma completa, profesional e imparcial una auditoría sobre la aplicación Lotus Notes instalada en cualquier organización, estas preguntas deben englobar todos los riesgos evaluados en el punto 6.2 del presente proyecto final de carrera, también indicaremos cuál es la finalidad de cada pregunta dentro del formulario y en relación a la auditoría.

Cuál es el nombre completo del entrevistado. La finalidad de esta pregunta es únicamente conocer al entrevistado.

Cuál es el trabajo que desempeña el entrevistado dentro de la organización y qué funciones y responsabilidades tiene el entrevistado dentro de la organización. La finalidad de esta pregunta es conocer las funciones del entrevistado dentro de la organización.

Cuánto tiempo lleva desempeñando las funciones que realiza actualmente para la organización. La finalidad de esta pregunta es vislumbrar si el entrevistado puede encontrarse desilusionado o estancado con su actual situación dentro de la organización.

Es empleado directo de la organización o si por el contrario pertenece a alguna otra organización que presta servicios en la organización auditada. La

finalidad de esta pregunta es saber si el entrevistado será más o menos sincero en sus respuestas.

Cuánto tiempo lleva trabajando el entrevistado para la organización y si siempre ha trabajado en ese centro. La finalidad de esta pregunta es poder conocer el nivel de implicación del entrevistado con la organización.

Cuándo fue la última vez que fue promocionado dentro de la organización. La finalidad de esta pregunta es vislumbrar si el entrevistado puede encontrarse desilusionado con su actual situación dentro de la organización.

Es necesario utilizar alguna identificación para acceder al centro de trabajo o si es necesaria alguna llave, tarjeta magnética, ficha,...La finalidad de esta pregunta es conocer si el acceso al edificio está restringido sólo al personal autorizado.

Para acceder a la oficina es necesario utilizar alguna identificación o llave. La finalidad de esta pregunta es conocer si el acceso a la oficina, en la que se encuentran los equipos informáticos, está restringido sólo al personal autorizado.

Para acceder al centro de cálculo en el que se encuentran los servidores es necesaria algún tipo de identificación o llave. La finalidad de esta pregunta es conocer si el acceso a la sala en la que se encuentran los servidores de la organización está restringido sólo al personal autorizado.

Qué usuario utiliza para acceder a los equipos informáticos. La finalidad de esta pregunta es conocer si se accede a los equipos informáticos con usuarios genéricos o si por el contrario cada empleado de la organización tiene su propio usuario.

Qué usuario utiliza para conectarse a la aplicación Lotus Notes. La finalidad de esta pregunta es conocer si el acceso a la aplicación Lotus Notes se hace con un usuario genérico o si cada miembro de la organización tiene el suyo propio.

Utiliza la misma contraseña para conectarse a los equipos informáticos que para conectarse a la aplicación Lotus Notes. La finalidad de esta pregunta es conocer si se usan diferentes contraseñas para el acceso a los equipos informáticos y para la aplicación Lotus Notes, puesto que si usa la misma contraseña podría tenerlas sincronizadas.

Utiliza el mismo usuario para conectarse a los equipos informáticos que para conectarse a la aplicación Lotus Notes. La finalidad de esta pregunta es conocer si se utilizan diferentes usuarios para conectarse a los equipos informáticos y a la aplicación Lotus Notes.

Cuándo fue la última vez que cambio la contraseña de acceso a su equipo informático. La finalidad de esta pregunta es conocer si se cambian las contraseñas de acceso a los equipos informáticos y si se cumplen los plazos de cambios de contraseña marcados por la normativa de la organización.

Cuándo fue la última vez que cambio la contraseña de acceso a la aplicación Lotus Notes. La finalidad de esta pregunta es conocer si se cambian las contraseñas de acceso a la aplicación Lotus Notes y si se cumplen los plazos de cambios de contraseña marcados por la normativa de la organización.

Cuando abandona su equipo informático lo deja bloqueado. La finalidad de esta pregunta es conocer si los empleados de la organización bloquean sus equipos cuando los dejan desatendidos para que no sean utilizados por otro empleado de la organización.

Cuándo abandona su equipo informático, bloquea la aplicación Lotus Notes. La finalidad de esta pregunta es conocer si los empleados de la organización bloquean la aplicación Lotus Notes cuando dejan desatendidos los equipos informáticos para que no sea utilizada por otro empleado de la organización

Siempre utiliza el mismo equipo informático. La finalidad de esta pregunta es conocer si los empleados tienen un equipo informático de trabajo fijo o si por el contrario utilizan el primero que quede libre.

Siempre que accede a la aplicación Lotus Notes lo hace siempre desde el mismo equipo informático. La finalidad de esta pregunta es conocer si los empleados tienen un equipo informático de trabajo fijo o si por el contrario utilizan el primero que quede libre.

Dónde se encuentra el equipo informático que habitualmente utiliza. La finalidad de esta pregunta es conocer las diferentes salas en las que se encuentran los equipos informáticos de la organización.

Los archivos temporales generados por la aplicación Lotus Notes son eliminados. La finalidad de esta pregunta es conocer si los archivos temporales generados durante la ejecución de la aplicación Lotus Notes son eliminados.

Con qué frecuencia se eliminan los archivos temporales generados por la aplicación Lotus Notes. La finalidad de esta pregunta es conocer la frecuencia de borrado de los ficheros temporales generados por la aplicación Lotus Notes durante su ejecución y si el borrado es manual o automático.

La eliminación de archivos temporales se hace de forma automática o manual. La finalidad de esta pregunta no es otra que saber de qué forma se eliminan los archivos temporales generados por la aplicación Lotus Notes.

Cifran la información almacenada en la aplicación Lotus Notes. La finalidad de esta pregunta es conocer si la información almacenada en la aplicación Lotus Notes es accesible por otros usuarios.

De qué forma cifran la información almacenada en la aplicación Lotus Notes. La finalidad de esta pregunta es conocer si los empleados de la organización conocen la opción de cifrado de la aplicación Lotus Notes y si la utilizan.

Al enviar correos lo hacen con acuse de recibo. La finalidad de esta pregunta es conocer si los empleados de la organización al enviar correos electrónicos con la aplicación Lotus Notes marcan la opción de acuse de recibo, que aparece en opciones de envío.

Los correos electrónicos que envían van con firma electrónica. La finalidad de esta pregunta es conocer si los correos electrónicos enviados mediante la aplicación Lotus Notes se envían con firma electrónica.

Los correos electrónicos que envían son codificados o no. La finalidad de esta pregunta es conocer si el envío de correo electrónico se hace de forma segura.

Preguntaremos si los correos electrónicos se envían a través de SSL. La finalidad de esta pregunta es, al igual que en el caso anterior, conocer si el envío de correos electrónicos se hace de forma segura.

Al recibir correos con adjuntos los abren directamente, independientemente de quién sea el remitente del correo y si este viene firmado o no. La finalidad de esta pregunta es conocer si abren directamente los correos adjuntos o si por el contrario primero verifican si se el adjunto puede contener algún tipo de virus.

Al abrir los correos recibidos pueden ver todas las imágenes incrustadas en el texto, o si por el contrario tienen que abrirlas expresamente. La finalidad de esta pregunta es conocer si la opción de la aplicación Lotus Notes *no mostrar imágenes remotas sin permiso*, para evitar posibles infecciones por virus informáticos.

Qué estructura de carpetas de correo utiliza para guardar los correos recibidos y enviados. La finalidad de esta pregunta es conocer si se siguen las políticas de archivado de correos electrónicos de la organización.

Qué tipo de plantillas de envío y contestación de correo electrónico utiliza. La finalidad de esta pregunta es conocer si se siguen las políticas de envío y contestación de correos electrónicos de la organización.

Qué tipo de licencia tiene la aplicación Lotus Notes y qué caducidad tiene dicha licencia. La finalidad de esta pregunta es saber si se está utilizando una licencia parcial o completa de la aplicación Lotus Notes y saber si se conoce la fecha de caducidad de la misma.

Se hacen copias de seguridad de los contenidos de la aplicación Lotus Notes de todos los usuarios o sólo de algunos. La finalidad de esta pregunta es conocer si se realizan copias de seguridad de los correos y libretas de direcciones de los empleados de la organización, para comprobar si se respetan las políticas de backup de la organización.

Cada cuanto tiempo se realizan las copias de seguridad de los contenidos de la aplicación Lotus Notes. La finalidad de esta pregunta es conocer si se respetan los plazos entre copias de seguridad reflejados en las políticas de la organización.

En qué formato se guardan las copias de seguridad de los contenidos de la aplicación Lotus Notes. La finalidad de esta pregunta es conocer en qué forma se almacenan las copias de seguridad, para saber si se cumple la normativa interna de la organización al respecto.

En qué lugar se almacenan las copias de seguridad de los contenidos de la aplicación Lotus Notes. La finalidad de esta pregunta es conocer en qué lugar se almacenan las copias de seguridad, para saber si se cumple la normativa interna de la organización al respecto.

Ahora mostraremos un ejemplo del formato que deberían tener los diferentes formularios.

<table>
<tr><td colspan="3">Identificador de cuestionario.</td><td>FECHA</td></tr>
<tr><td>Entrevistador:</td><td>Nombre</td><td>Apellidos</td><td>Firma</td></tr>
<tr><td>Entrevistado:</td><td>Nombre</td><td>Apellidos</td><td>Firma</td></tr>
<tr><td colspan="4">Primera pregunta</td></tr>
<tr><td colspan="4">Primera respuesta</td></tr>
<tr><td colspan="4">Segunda pregunta</td></tr>
<tr><td>SI</td><td>NO</td><td colspan="2">NO APLICABLE</td></tr>
</table>

Tercera pregunta		
SI	NO	NO SABE NO CONTESTA
….		
Pregunta enésima		
Respuesta enésima		

Figura 6.16: Ejemplos de cuestionario genérico.

A continuación mostraremos 3 ejemplos de cuestionarios, uno para cada uno de los diferentes tipos de usuarios que entrevistaremos.

Ejemplo de cuestionario de usuario principiante de la aplicación Lotus Notes, pero sin incluir los espacios de las respuestas.

Identificador de cuestionario.			FECHA
Entrevistador:	Nombre	Apellidos	Firma
Entrevistado:	Nombre	Apellidos	Firma
¿Qué tipo de trabajo desempeña?			

¿Cuánto tiempo lleva realizando su trabajo actual?
¿Está contratado por la organización de forma directa?
¿Cuánto tiempo lleva trabajando para la organización?
¿Cuándo fue la última vez que fue promocionado?
¿Es necesario algún tipo de identificación para acceder al centro de trabajo?
¿Es necesario algún tipo de identificación para acceder a la oficina?
¿Qué usuario utiliza para acceder a los equipos informáticos?
¿Qué usuario utiliza para acceder a la aplicación Lotus Notes?
¿Utiliza la misma contraseña para acceder a los equipos informáticos que para acceder a la aplicación Lotus Notes?
¿Utiliza el mismo usuario para acceder a los equipos informáticos que para acceder a la aplicación Lotus Notes?
¿Cuándo fue la última vez que cambió la contraseña de acceso a la aplicación Lotus Notes?
¿Cuándo fue la última vez que cambió la contraseña de acceso a los equipos informáticos?

¿Cuando deja de utilizar su equipo informático bloquea la aplicación Lotus Notes?
¿Cuando deja de utilizar su equipo informático lo bloquea?
¿Dónde se encuentra su equipo informático?
¿Al enviar correos electrónicos los firma con algún tipo de firma electrónica?
¿Al enviar correos electrónicos lo hace de forma codificada?
¿Al recibir correos con ficheros adjuntos los abre siempre, o sólo los de algunos remitentes?
¿Al recibir correos con imágenes incrustadas las puede ver sin realizar ninguna acción previa?
¿Qué estructura de carpetas utiliza para almacenar los correos enviados y recibidos?
¿Qué tipo de plantillas utiliza para responder y enviar correos?

Figura 6.17.: Ejemplo de cuestionario para usuario principiante.

Ejemplo de cuestionario de usuario avanzado de la aplicación Lotus Notes, pero sin incluir los espacios de las respuestas.

Identificador de cuestionario.			FECHA
Entrevistador:	Nombre	Apellidos	Firma
Entrevistado:	Nombre	Apellidos	Firma
¿Qué tipo de trabajo desempeña?			
¿Cuánto tiempo lleva realizando su trabajo actual?			
¿Está contratado por la organización de forma directa?			
¿Cuánto tiempo lleva trabajando para la organización?			
¿Cuándo fue la última vez que fue promocionado?			
¿Es necesario algún tipo de identificación para acceder al centro de trabajo?			
¿Es necesario algún tipo de identificación para acceder a la oficina?			

¿Qué usuario utiliza para acceder a los equipos informáticos?
¿Qué usuario utiliza para acceder a la aplicación Lotus Notes?
¿Utiliza la misma contraseña para acceder a los equipos informáticos que para acceder a la aplicación Lotus Notes?
¿Utiliza el mismo usuario para acceder a los equipos informáticos que para acceder a la aplicación Lotus Notes?
¿Cuándo fue la última vez que cambió la contraseña de acceso a la aplicación Lotus Notes?
¿Cuándo fue la última vez que cambió la contraseña de acceso a los equipos informáticos?
¿Cuando deja de utilizar su equipo informático bloquea la aplicación Lotus Notes?
¿Cuando deja de utilizar su equipo informático lo bloquea?
¿Utiliza distintos equipos informáticos?
¿Siempre accede a la aplicación Lotus Notes desde el mismo equipo informático?
¿Dónde se encuentra su equipo informático?
¿Codifica toda la información almacenada en su usuario de la aplicación Lotus Notes?

¿Cómo realiza la codificación de la información almacenada en la aplicación Lotus Notes?
¿Realiza envíos de correo con acuse de recibo?
¿Al enviar correos electrónicos los firma con algún tipo de firma electrónica?
¿Al enviar correos lo hace de forma codificada?
¿Al enviar correos electrónicos lo hace mediante SSL?
¿Al recibir correos con ficheros adjuntos los abre siempre, o sólo los de algunos remitentes?
¿Al recibir correos con imágenes incrustadas las puede ver sin realizar ninguna acción previa?
¿Qué estructura de carpetas utiliza para almacenar los correos enviados y recibidos?
¿Qué tipo de plantillas utiliza para responder y enviar correos?

Figura 6.18: Ejemplo de formulario para usuario avanzado.

Ejemplo de cuestionario de administrador de la aplicación Lotus Notes, pero sin incluir los espacios de las respuestas.

Identificador de cuestionario.			FECHA
Entrevistador:	Nombre	Apellidos	Firma
Entrevistado:	Nombre	Apellidos	Firma
¿Qué tipo de trabajo desempeña?			
¿Cuánto tiempo lleva realizando su trabajo actual?			
¿Está contratado por la organización de forma directa?			
¿Cuánto tiempo lleva trabajando para la organización?			
¿Cuándo fue la última vez que fue promocionado?			
¿Es necesario algún tipo de identificación para acceder al centro de trabajo?			
¿Es necesario algún tipo de identificación para acceder a la oficina?			

¿Es necesario algún tipo de identificación para acceder a la sala en la que se encuentran los servidores de la aplicación Lotus Notes?
¿Utiliza la misma contraseña para acceder a los equipos informáticos que para acceder a la aplicación Lotus Notes?
¿Utiliza el mismo usuario para acceder a los equipos informáticos que para acceder a la aplicación Lotus Notes?
¿Cuando deja de utilizar su equipo informático bloquea la aplicación Lotus Notes?
¿Cuando deja de utilizar su equipo informático lo bloquea?
¿Los archivos temporales generados por la aplicación Lotus Notes son eliminados?
¿Cada cuánto tiempo se eliminan los archivos temporales generados por la aplicación Lotus Notes?
¿Los archivos temporales de Lotus Notes se eliminan de forma automática?
¿La información almacenada en la aplicación Lotus Notes se codifica?
¿Cómo realiza la codificación de la información almacenada en la aplicación Lotus Notes?
¿Qué tipo de licencia utiliza la aplicación Lotus Notes?
¿Qué caducidad tiene la licencia de la aplicación Lotus Notes?

¿Se realizan copias de seguridad de la información almacenada en la aplicación Lotus Notes?
¿De qué partes de la aplicación Lotus Notes se realizan las copias de seguridad y de qué usuarios?
¿Con qué frecuencia se realizan las copias de seguridad de la aplicación Lotus Notes?
¿En qué soporte se almacenan las copias de seguridad de la aplicación Lotus Notes?
¿En dónde se guardan las copias de seguridad de la aplicación Lotus Notes?

Figura 6.19.: Ejemplo de cuestionario de administrador.

7. PROTOTIPO DE APLICACIÓN DE CUESTIONARIOS.

7.1 INTRODUCCIÓN.

A lo largo de este punto mostraremos un posible prototipo de aplicación de cuestionarios.

Esta aplicación permite a los auditores y/o encuestadores realizar encuestas de forma dinámica a través de un equipo informático, en lugar de realizar dichas encuestas en papel.

De esta forma pretendemos ahorrar mucho tiempo en la consulta de las respuestas de los entrevistados y además no se genera tanta documentación en papel, lo que permite una mejor optimización de los recursos que la utilización de los medios tradicionales.

En primer lugar procederemos a enumerar los distintos perfiles de usuario que tendrá la aplicación y explicaremos por qué se han elegido estos perfiles y no otros. La aplicación tendrá tres tipos diferentes de usuarios: administrador, auditor y encuestador. Los administradores son los encargados de añadir, eliminar o modificar usuarios dentro de la aplicación, de esta forma se consigue una mayor seguridad de la aplicación, y también pueden realizar las mismas operaciones sobre los cuestionarios, esto es debido a que se puede dar el caso que algunos auditores, por el motivo que sea, no puedan realizar operaciones sobre alguno o varios cuestionarios, por lo que el administrador sería el encargado de realizar esas operaciones. Los auditores pueden añadir, eliminar o modificar cuestionarios, estas funciones recaen sobre los auditores,

porque ellos son los encargados de llevar a cabo las diferentes auditorías, por lo tanto son los encargados de crear la estructura y las preguntas de los diferentes cuestionarios. Los encuestadores son los encargados de realizar las preguntas a los entrevistados, pero no pueden realizar ninguna modificación posterior sobre los cuestionarios, de esta forma lo que pretendemos es una mayor seguridad de la aplicación debido a la segregación de funciones.

En principio la aplicación no impone ninguna restricción en cuanto a que un mismo usuario tenga varios perfiles, ya que una misma persona puede desempeñar diferentes funciones dentro de una auditoría, dependiendo de la estructura del grupo de trabajo.

En segundo lugar, cabe destacar que únicamente hemos realizado un prototipo de aplicación, por lo que simplemente, mostraremos la apariencia que debería tener la aplicación y cuál sería su funcionamiento, pero no mostraremos una aplicación que sea completa, ni que funcione ni permita introducir registros. La aplicación debería interactuar con una base de datos en la que se almacenaran todos los registros de los cuestionarios y de los usuarios.

Y por último podemos destacar que la elaboración del prototipo se ha llevado a cabo en Java Swing, utilizando para ello la herramienta de programación Netbeans.

7.2 PROTOTIPO.

A lo largo de este apartado mostraremos el funcionamiento que debería seguir la aplicación, para ello utilizaremos el prototipo realizado.

En primer lugar, para poder hacer uso de la aplicación los diferentes usuarios deben introducir su usuario y contraseña, para verificar que tienen acceso a la misma, tal y como se muestra en la siguiente figura.

Figura 7.1: Pantalla de acceso a la aplicación.

En el caso que el usuario tuviese diferentes perfiles, tras ser autenticado de forma correcta en la aplicación debería seleccionar el tipo de perfil con el que quiere comenzar su sesión actual, tal y como se muestra en la siguiente figura:

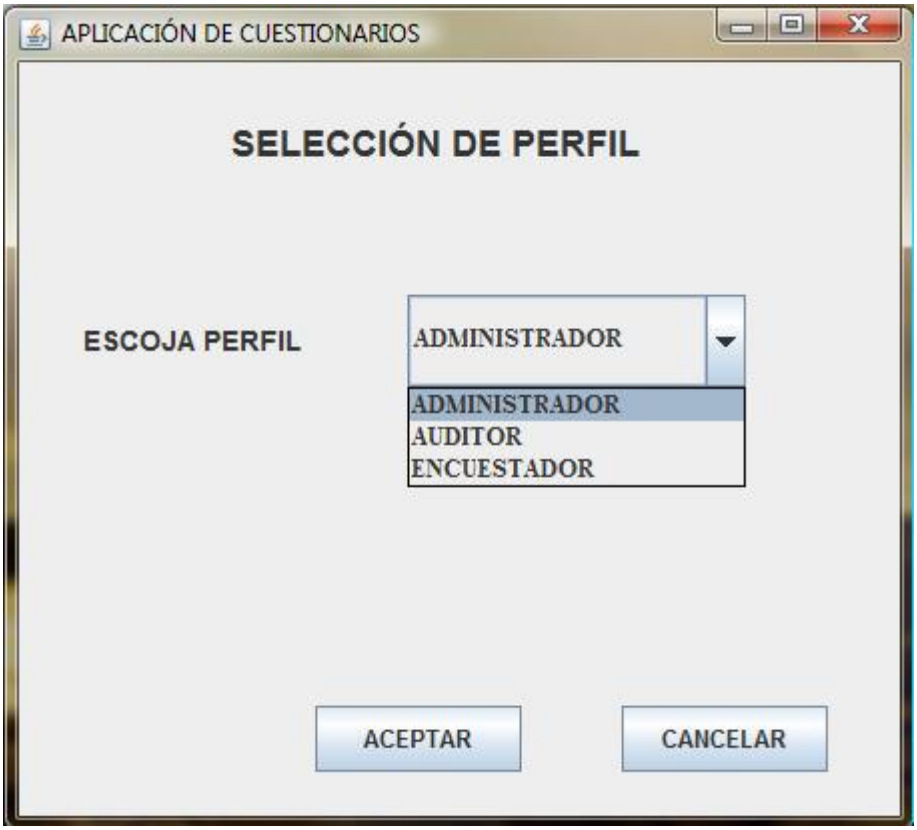

Figura 7.2: Pantalla de selección de perfil para la sesión actual.

Para el caso en que el usuario tuviese perfil de administrador y lo hubiese elegido, aparecería la pantalla de *administración usuarios* por defecto, aunque seleccionando en la pestaña de *cuestionarios* aparecería la *administración cuestionarios*, para la administración tanto de cuestionarios como de usuarios se puede añadir, eliminar, consultar y modificar, como se puede comprobar en las siguiente figuras.

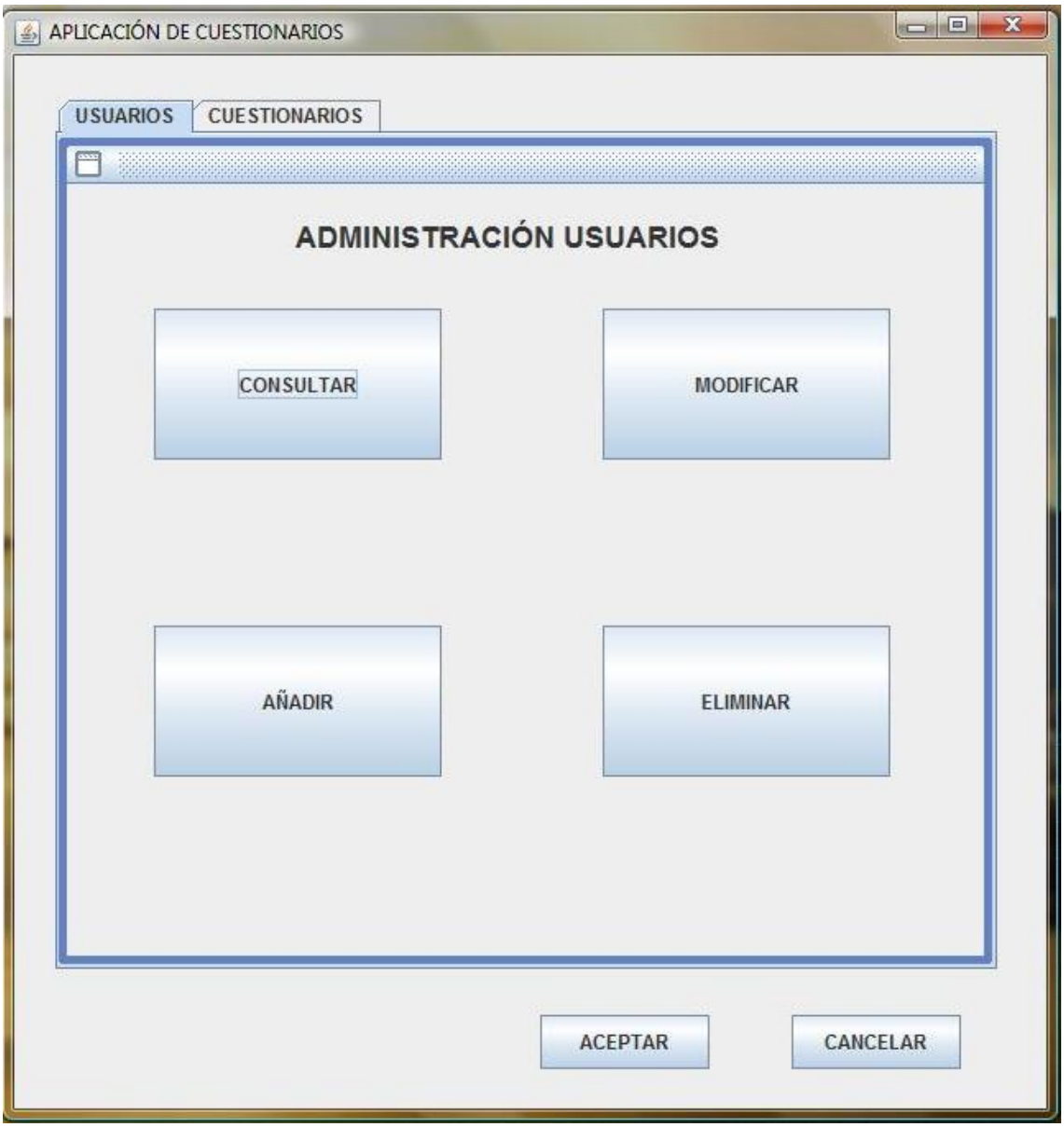

Figura 7.3: Pantalla de administración de usuarios.

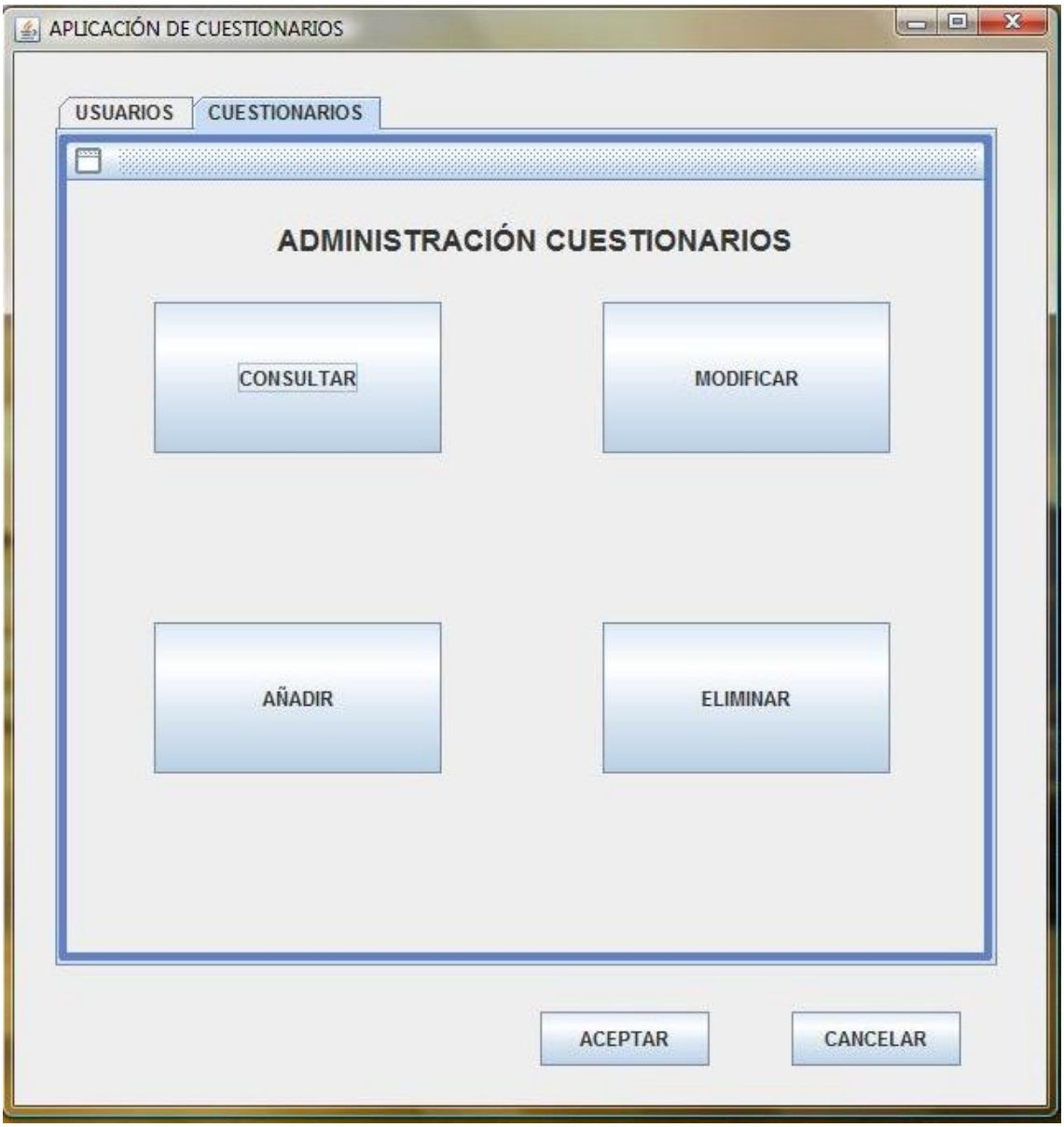

Figura 7.4: Pantalla de administración de cuestionarios.

Para el caso que se desease introducir un nuevo usuario en la aplicación se deberían introducir el nombre, apellidos, identificador y perfil o perfiles que tendría el nuevo usuario, tal y como se refleja en la siguiente figura.

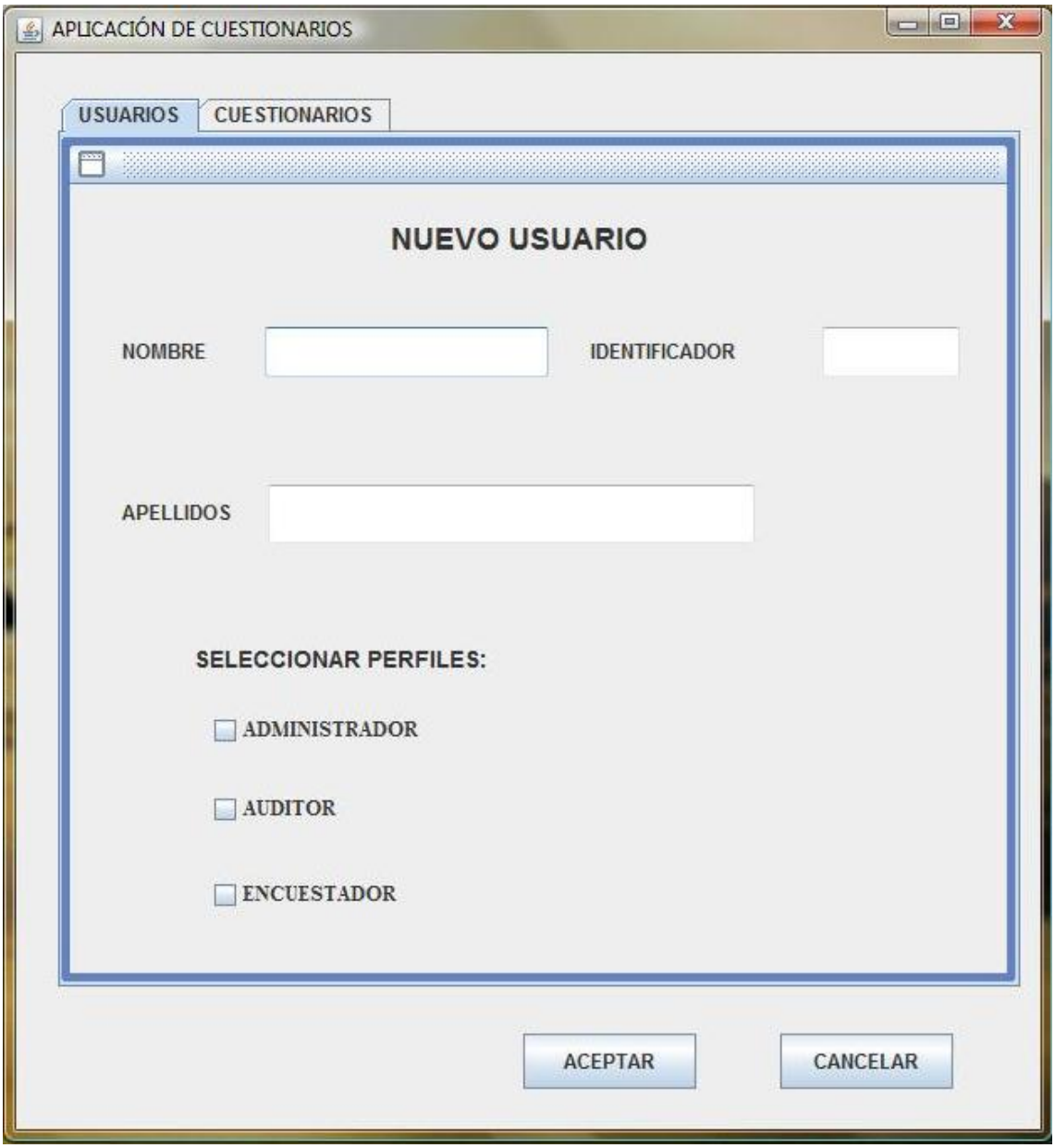

Figura 7.5: Pantalla de nuevo usuario.

A continuación mostraremos la pantalla de creación de cuestionario a la que tienen acceso tanto los administradores de la aplicación como los auditores, con la única salvedad, de que a estos últimos no les aparece la pestaña usuarios. Para introducir un nuevo cuestionario en la aplicación es obligatorio introducir el nombre del cuestionario, la fecha, el número de preguntas, el nombre de la

organización en la que se utilizará el cuestionario y una pequeña descripción del mismo, tal y como se puede ver en la siguiente figura.

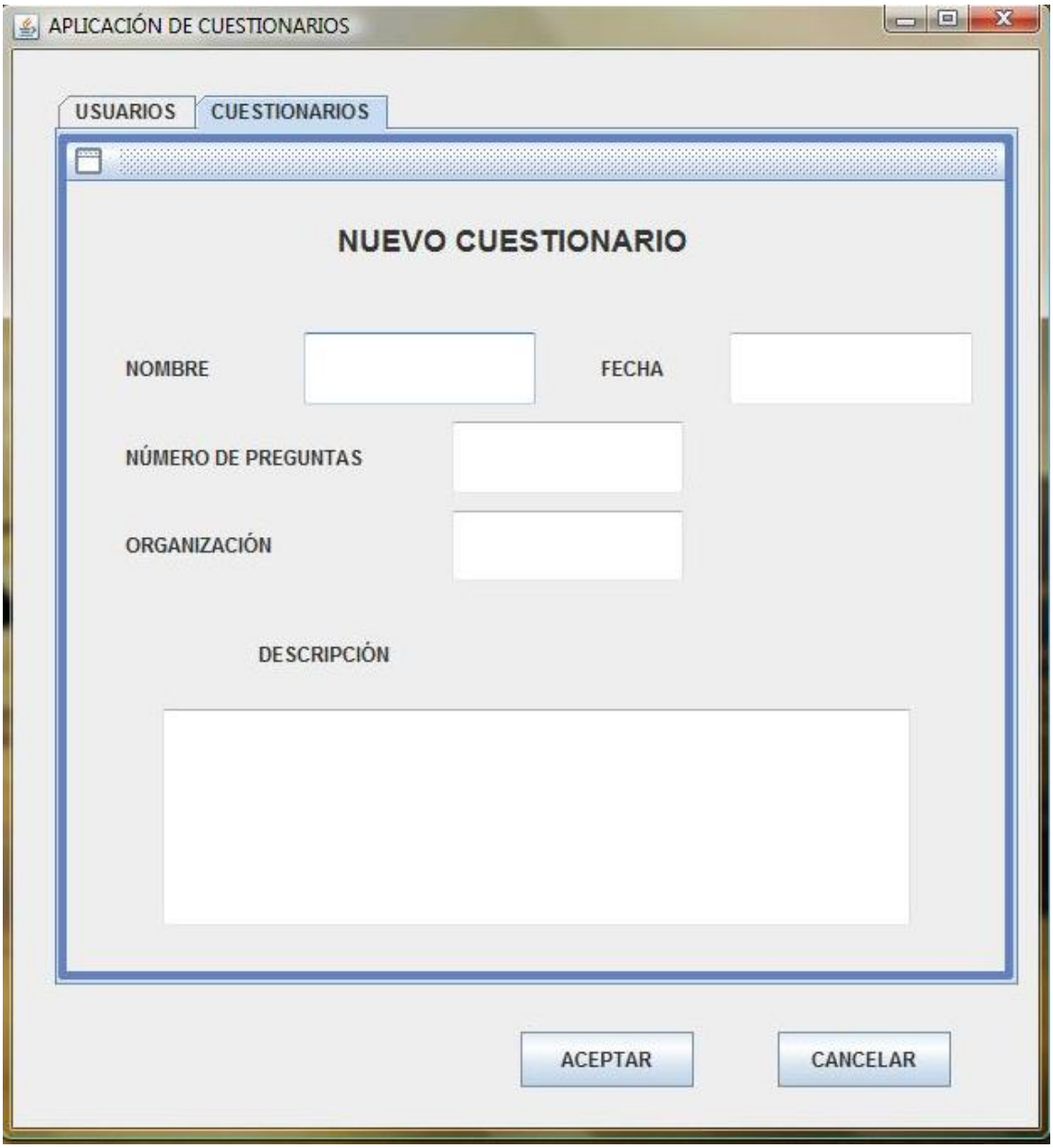

Figura 7.6: Pantalla de nuevo cuestionario.

Una vez que se ha creado un cuestionario el siguiente paso es vincular un auditor, para que pueda introducir las preguntas que se realizarán durante la auditoría, también se puede vincular un encuestador, que será el encargado de

realizar las entrevistas. Como se puede comprobar en la siguiente figura, permitimos que se añadan a la vez tanto auditores como encuestadores, esta pantalla es común tanto para administradores como para auditores, pero estos últimos sólo pueden incluir auditores y/o encuestadores en aquellos cuestionarios de los que son auditores, es decir, un auditor no puede introducirse como auditor de un cuestionario por sí sólo.

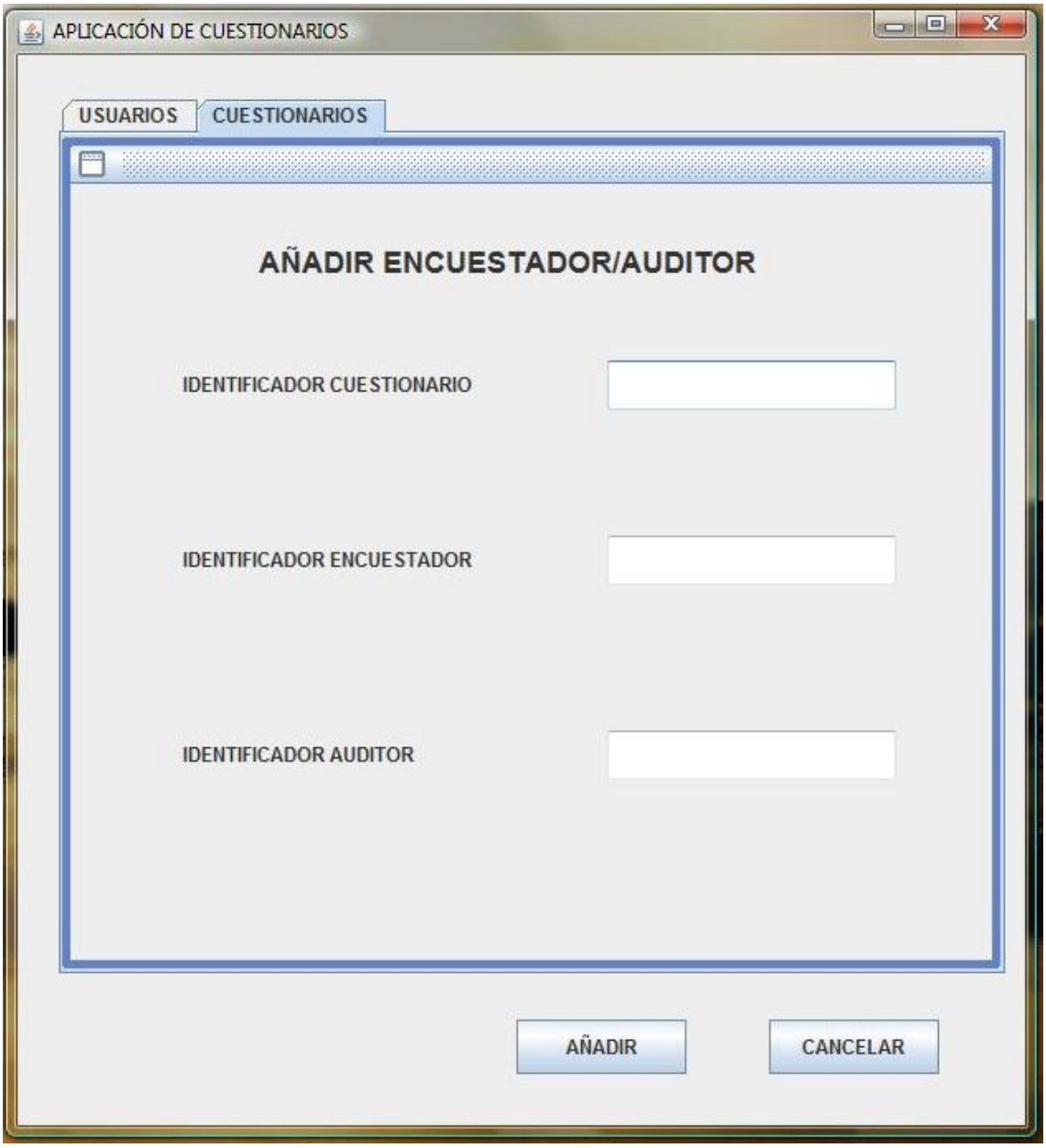

Figura 7.7: Pantalla de vinculación cuestionario auditor/encuestador.

A continuación mostraremos las pantallas de búsqueda de usuario y cuestionario, que básicamente son prácticamente iguales a las de modificación y eliminación, por este motivo no hemos creído necesario implementar las pantallas de modificación y eliminación de usuario y de cuestionario, ya que la única diferencia con las de búsqueda que si mostraremos será, que el nombre del botón izquierdo de la parte inferior en lugar, en lugar de poner buscar, pondría modificar o eliminar respectivamente.

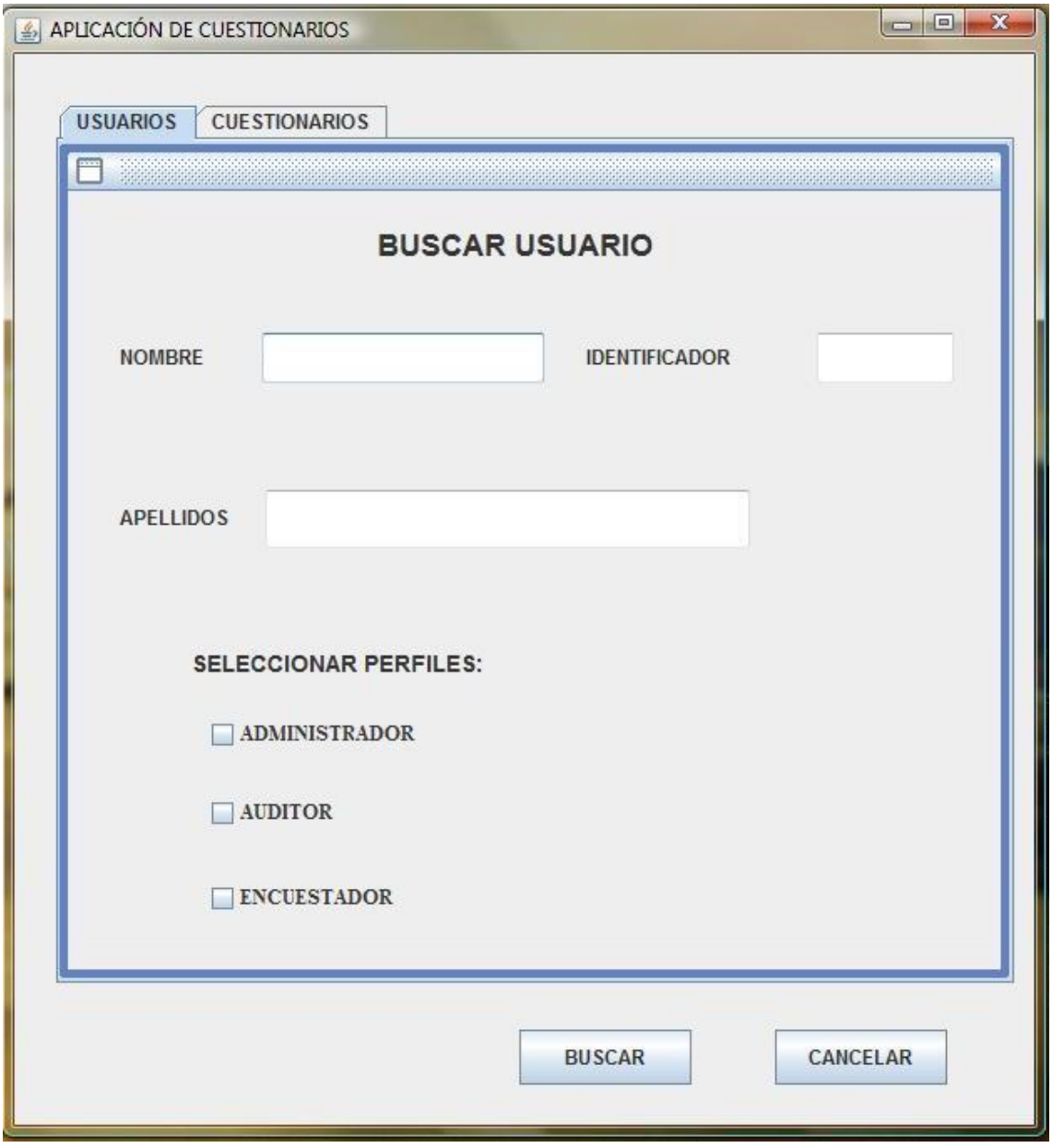

Figura 7.8: Pantalla de búsqueda de usuarios.

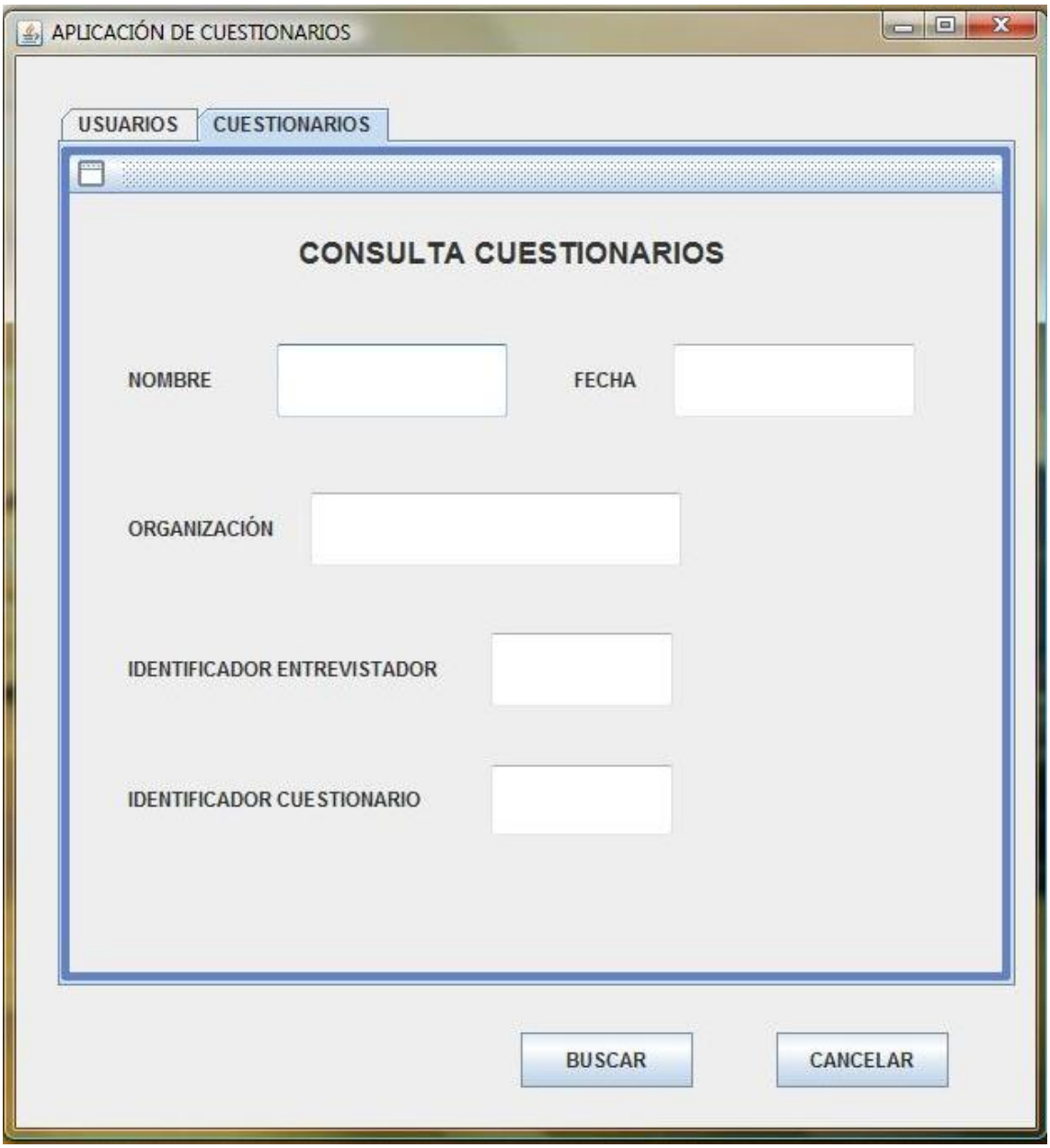

Figura 7.9: Pantalla de búsqueda de cuestionario.

Todos los campos reflejados tanto en la pantalla de búsqueda de usuarios como de búsqueda de cuestionarios son opcionales, y admiten expresiones regulares, de esta forma lo que se busca es una mayor flexibilidad de la búsqueda.

A continuación mostraremos la pantalla de comienzo de una entrevista y las pantallas de los diferentes tipos de pregunta que se contemplan en la aplicación.

En la pantalla de comienzo de cuestionario se deben introducir los datos de la persona entrevistada nombre y apellidos, la fecha y hora en la que se realizan la entrevista y el lugar en el que se llevará a cabo.

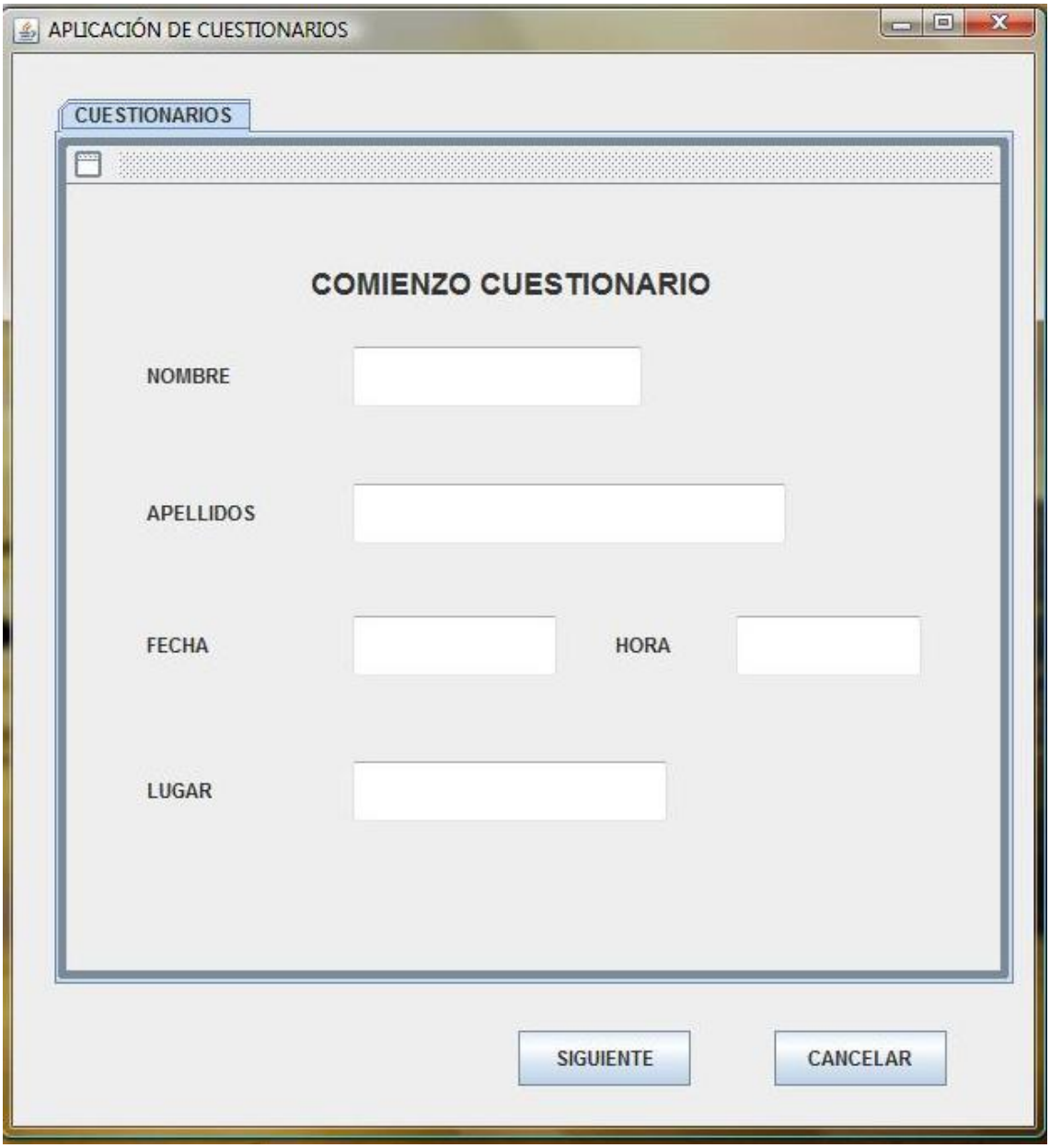

Figura 7.10: Pantalla de comienzo de cuestionario.

A continuación mostraremos un ejemplo de cómo sería una pregunta de respuesta simple, que además añade la opción de *No aplica* que será marcada en los casos en que la pregunta en cuestión dependa de la respuesta de la pregunta anterior.

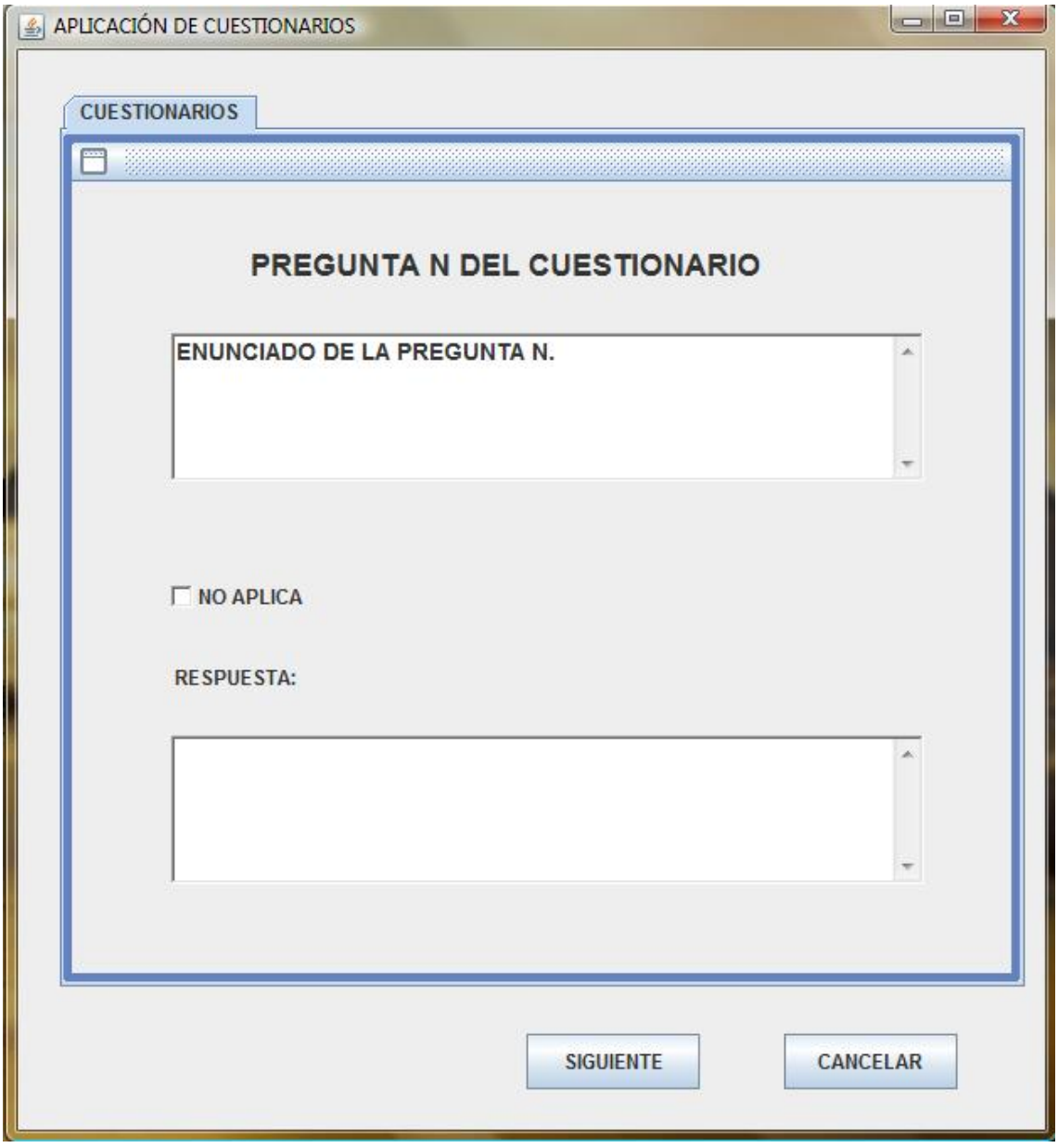

Figura 7.11: Pantalla de pregunta genérica.

Ahora mostraremos un ejemplo de pregunta concreta con las opciones *SI, NO* o *NO SABE, NO CONTESTA*, al igual que en el tipo anterior de pregunta aparece la opción *No aplica.*

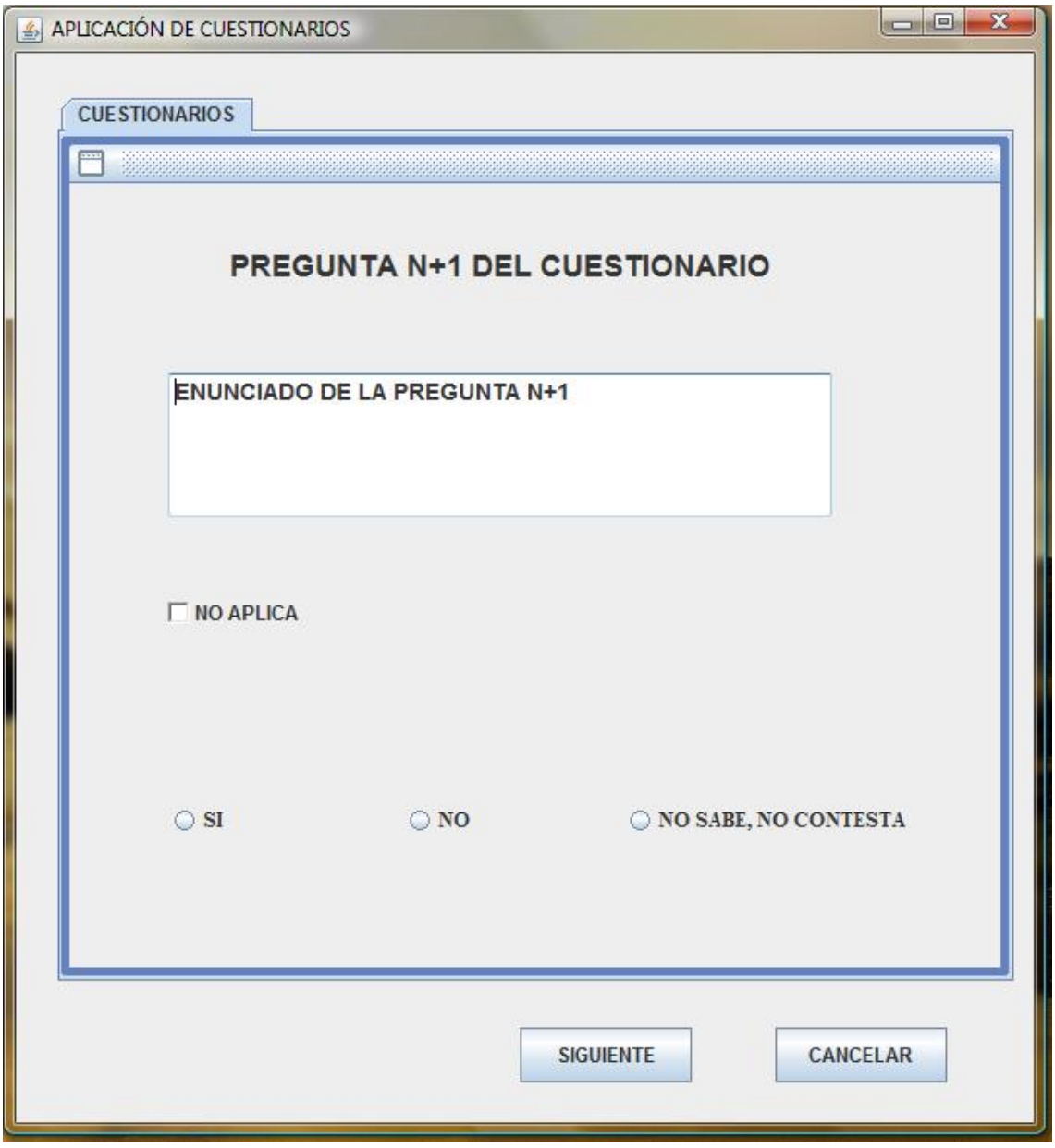

Figura 7.12: Pantalla de pregunta con respuesta SI-NO

Por último mostraremos un ejemplo de pregunta con múltiples opciones de respuesta, al igual que en los casos anteriores aparece la opción de *No aplica*.

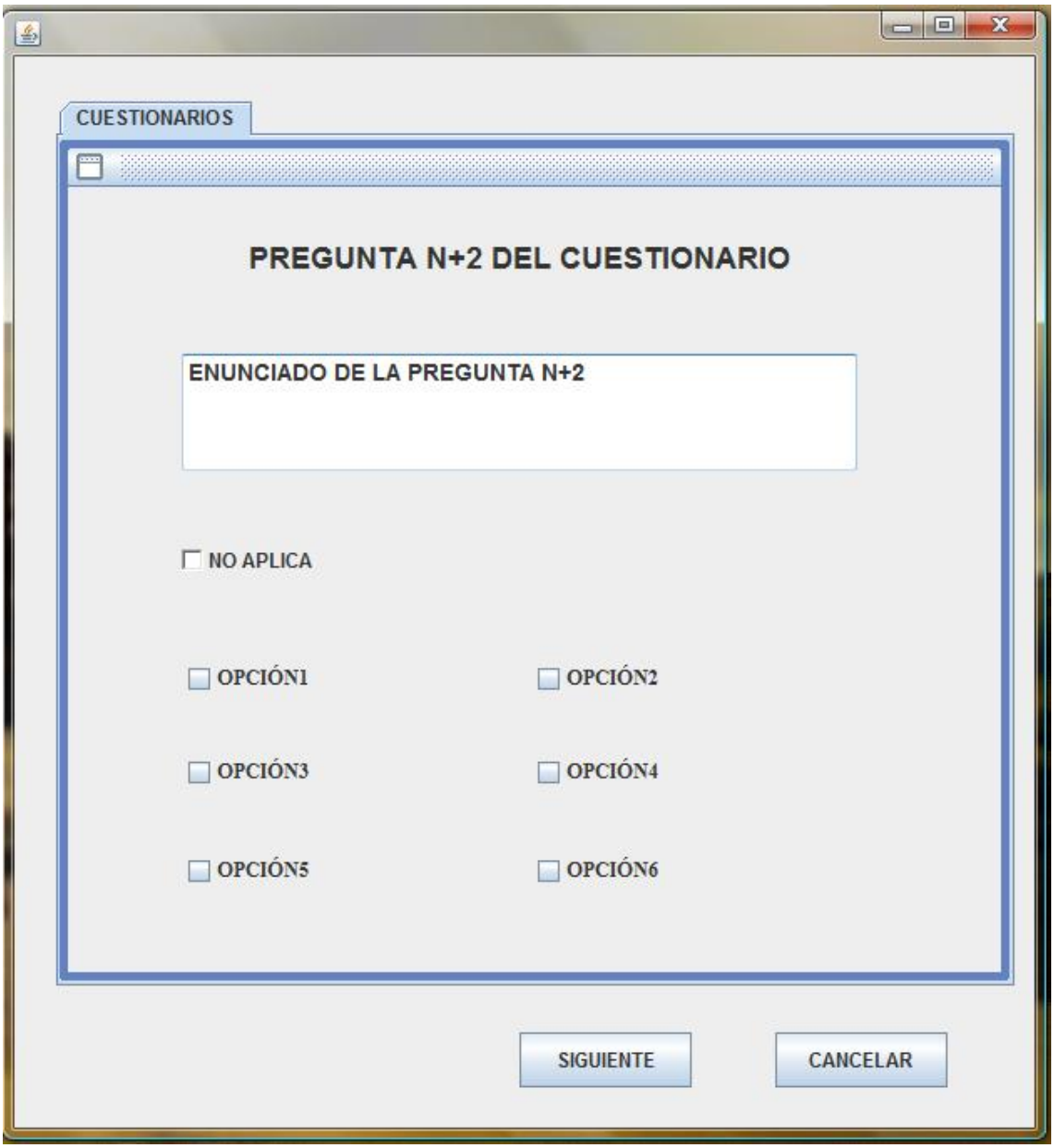

Figura 7.13: Pantalla de pregunta con multirespuesta.

7.3 EJEMPLO DE REALIZACIÓN DE CUESTIONARIO.

A lo largo de este apartado mostraremos un ejemplo de la realización de un cuestionario a un usuario principiante en la utilización de la aplicación Lotus Notes usando para dicho cuestionario la aplicación de cuestionarios descrita a lo largo de este punto:

El cuestionario comenzaría por la primera pregunta, tal y como se mostró en la figura 7.10, y seguidamente irían el resto de preguntas tal y como se puede comprobar en las siguientes figuras:

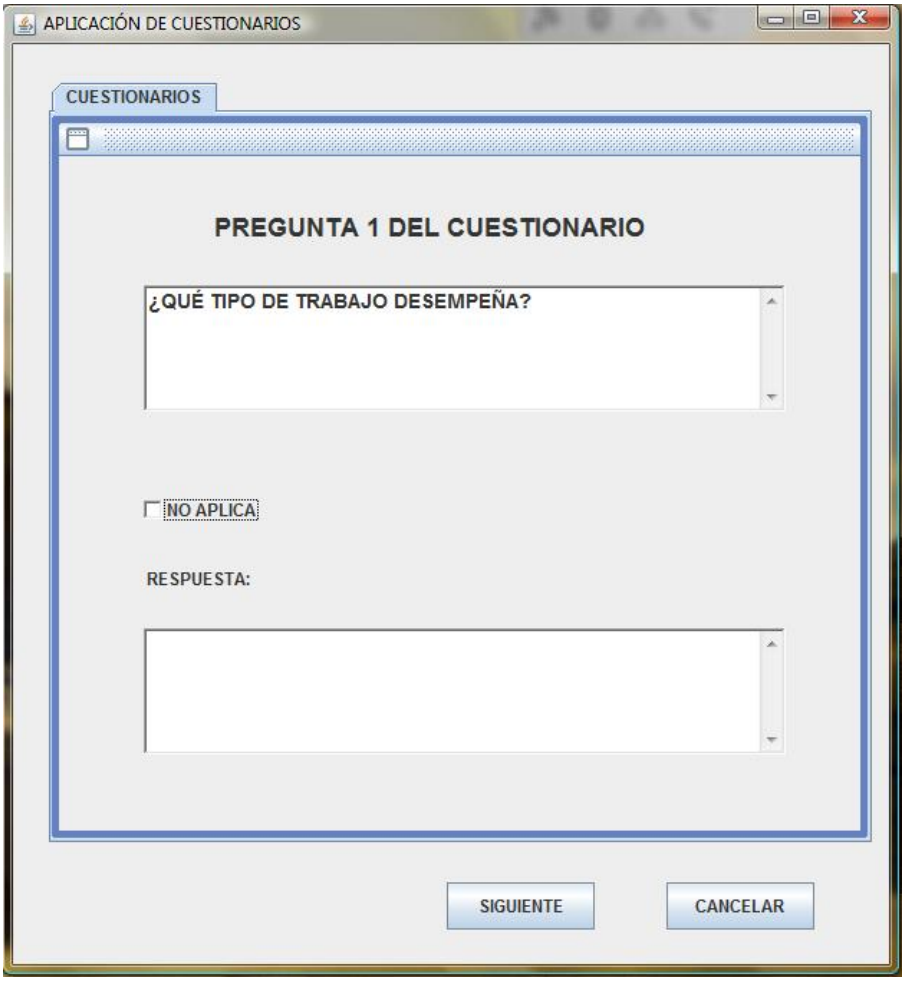

Figura 7.14: Pregunta 1del cuestionario.

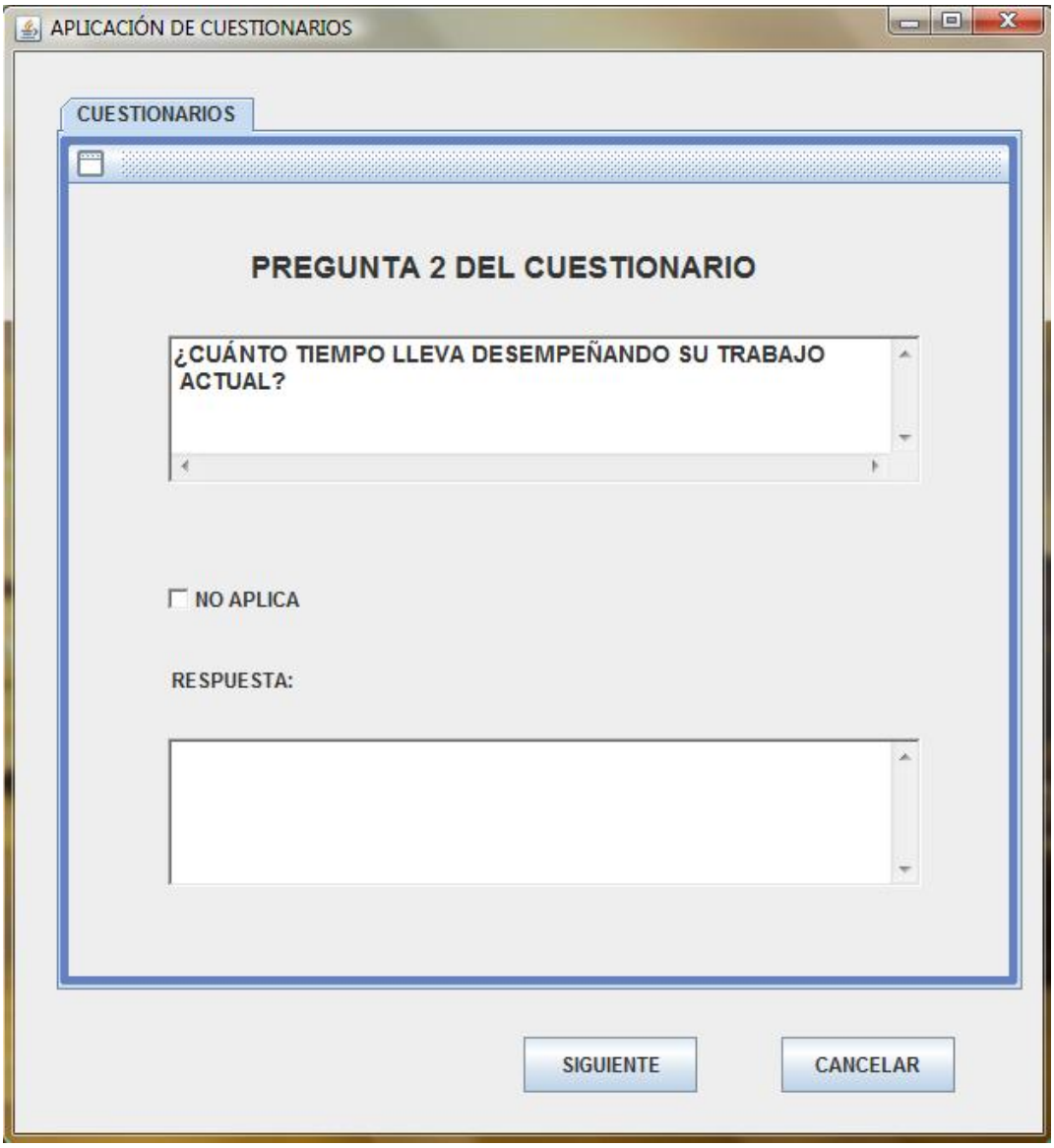

Figura 7.15: Pregunta 2 del cuestionario

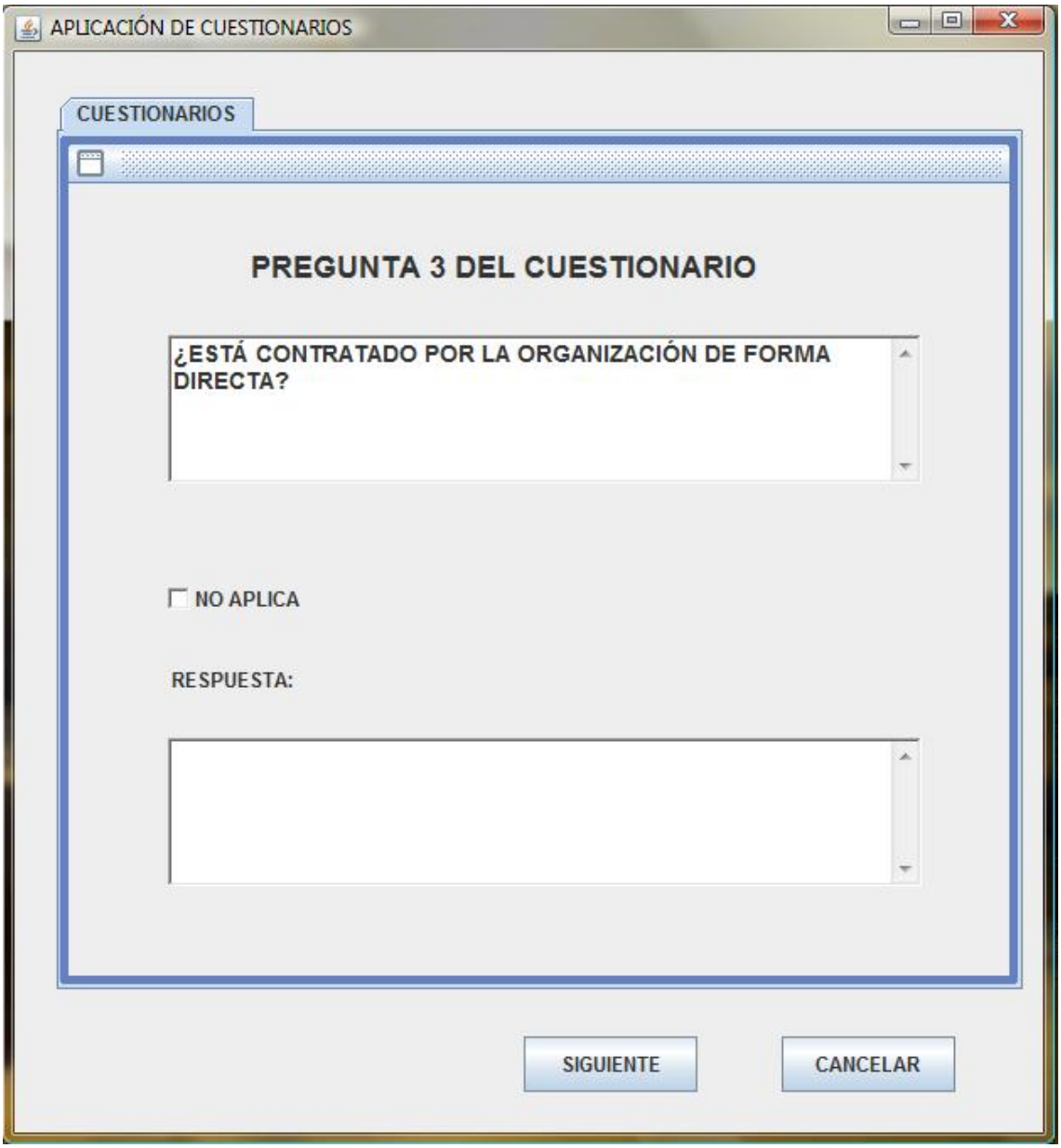

Figura 7.16: Pregunta 3 del cuestionario.

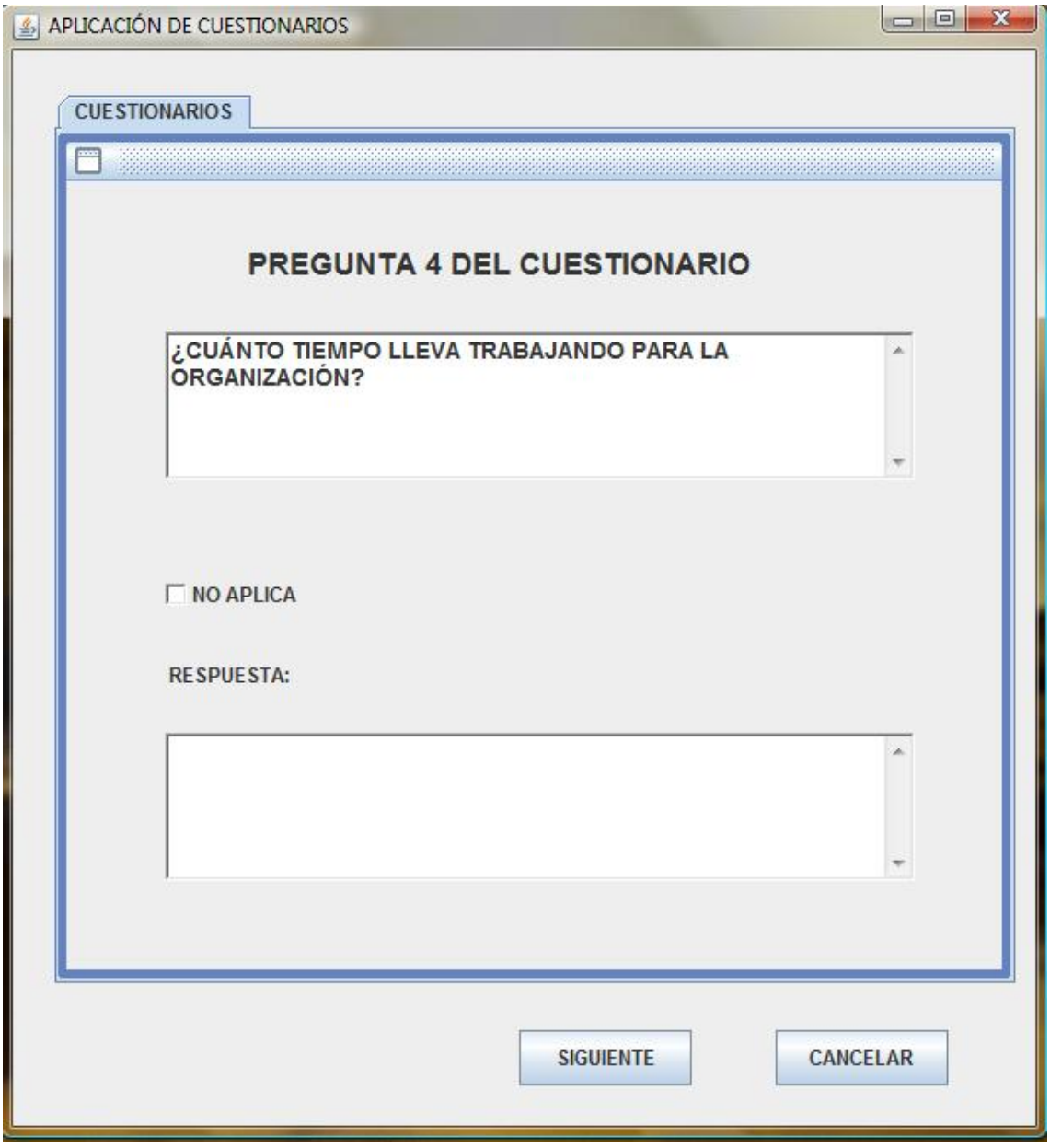

Figura 7.17: Pregunta 4 del cuestionario.

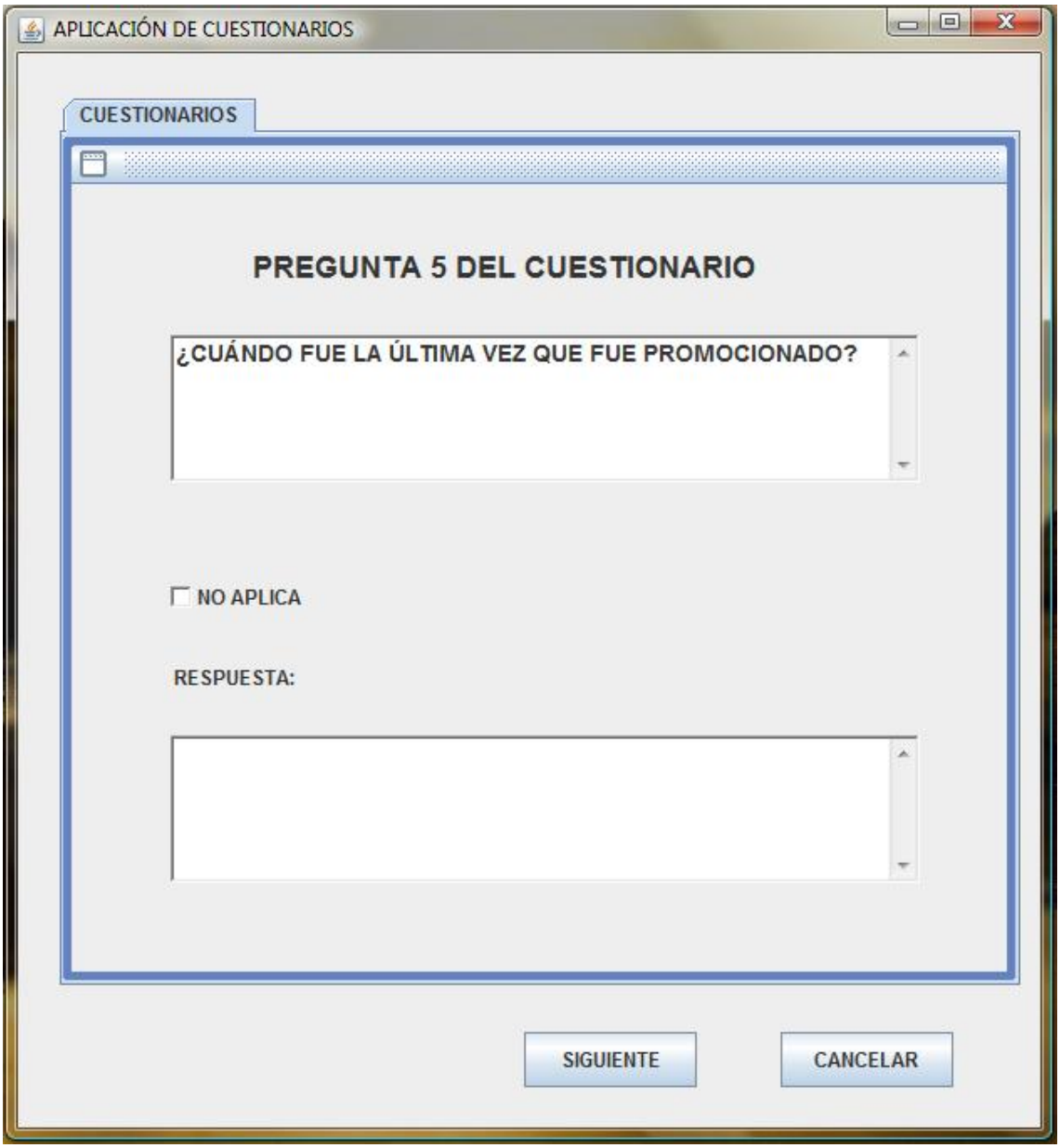

Figura 7.18: Pregunta 5 del cuestionario.

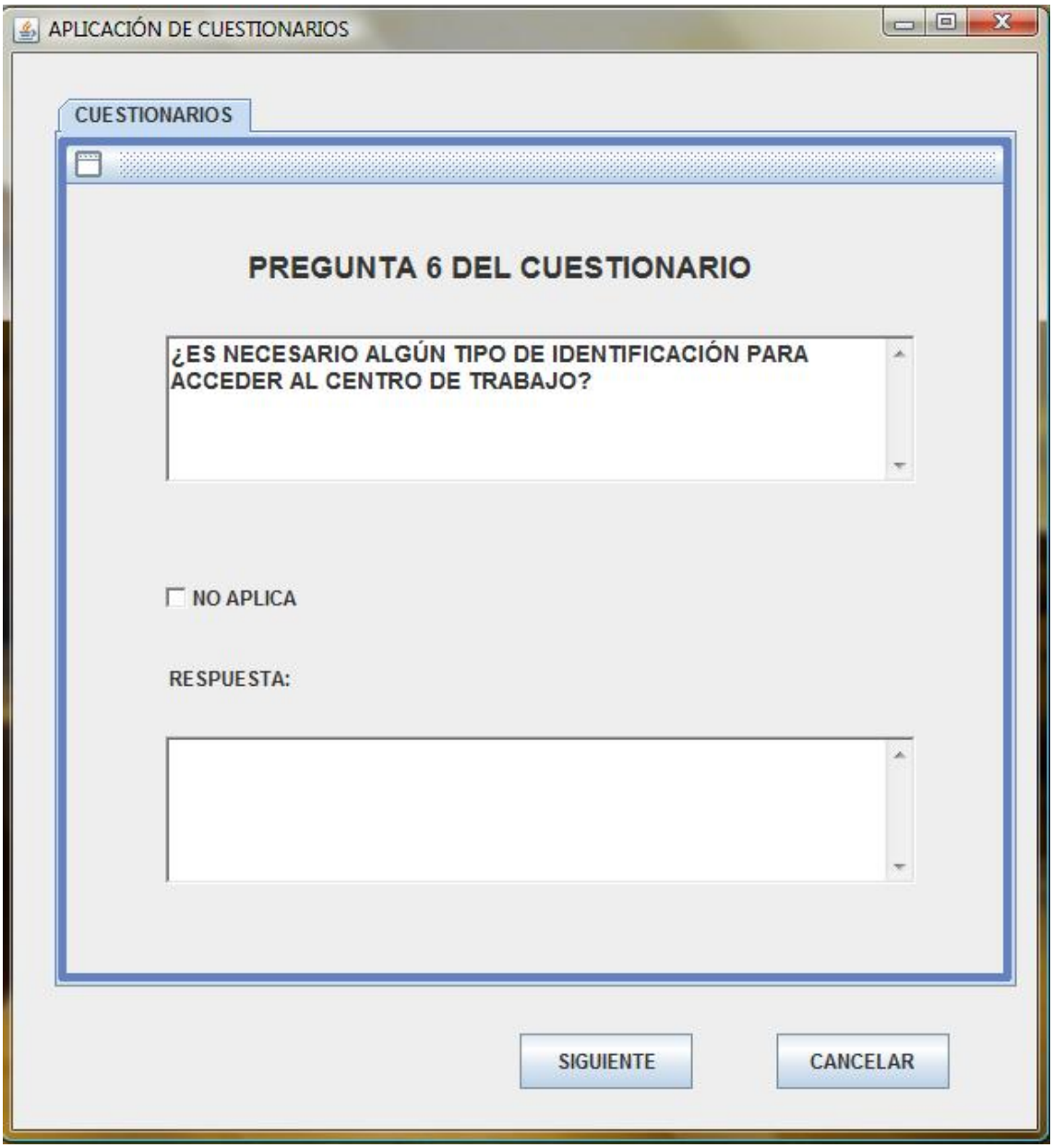

Figura 7.19: Pregunta 6 del cuestionario.

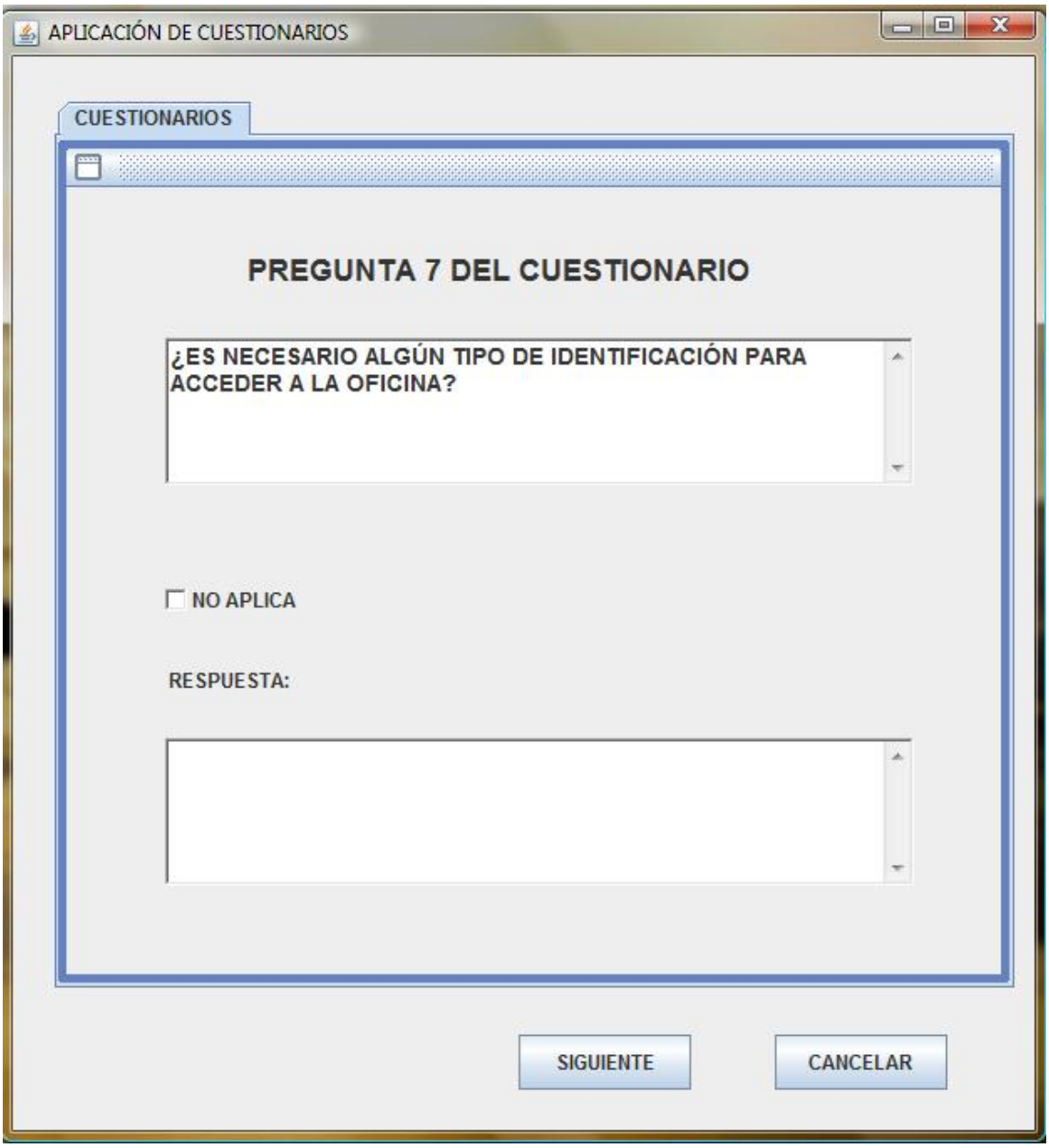

Figura 7.20: Pregunta 7 del cuestionario.

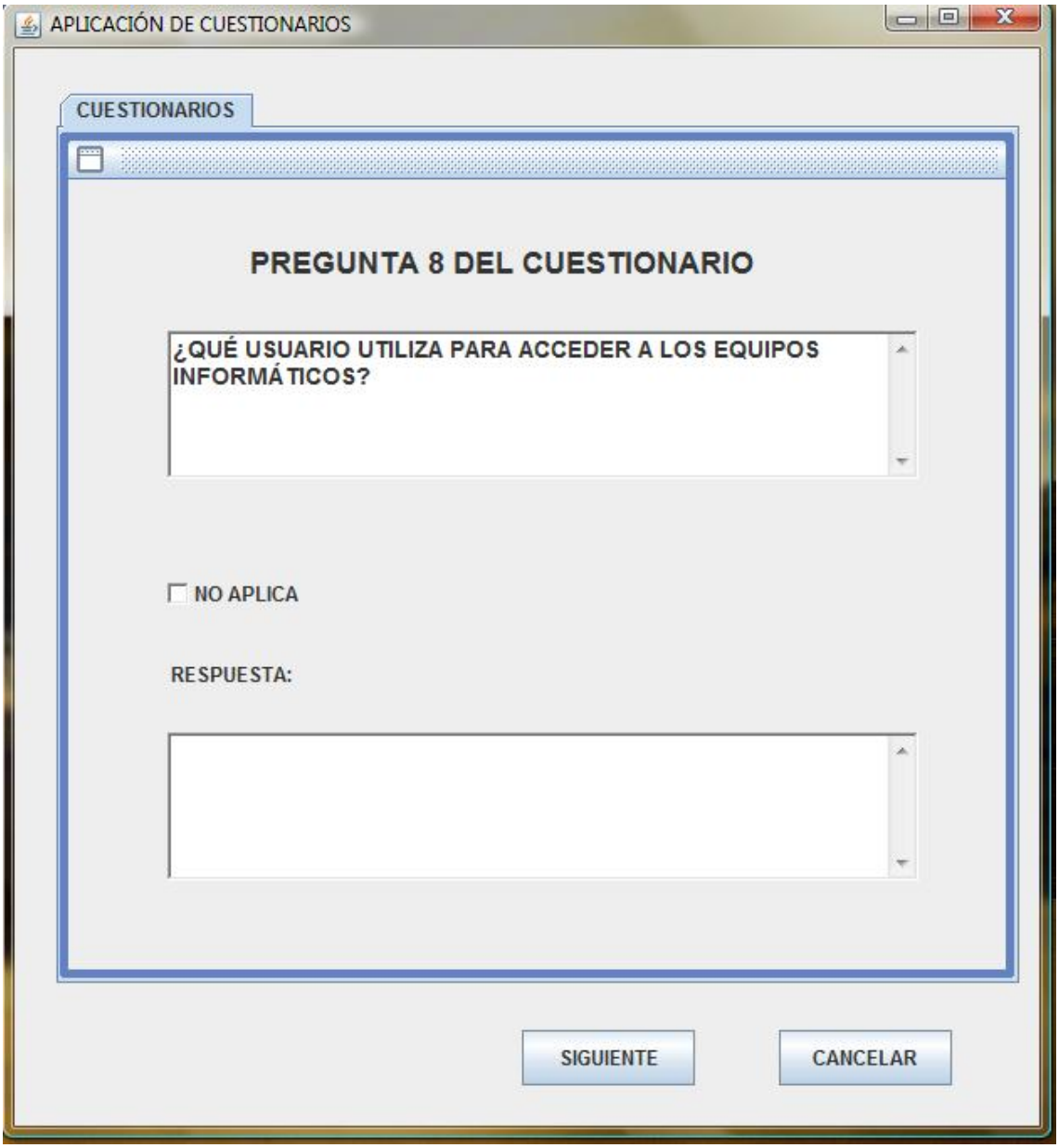

Figura 7.21: Pregunta 8 del cuestionario.

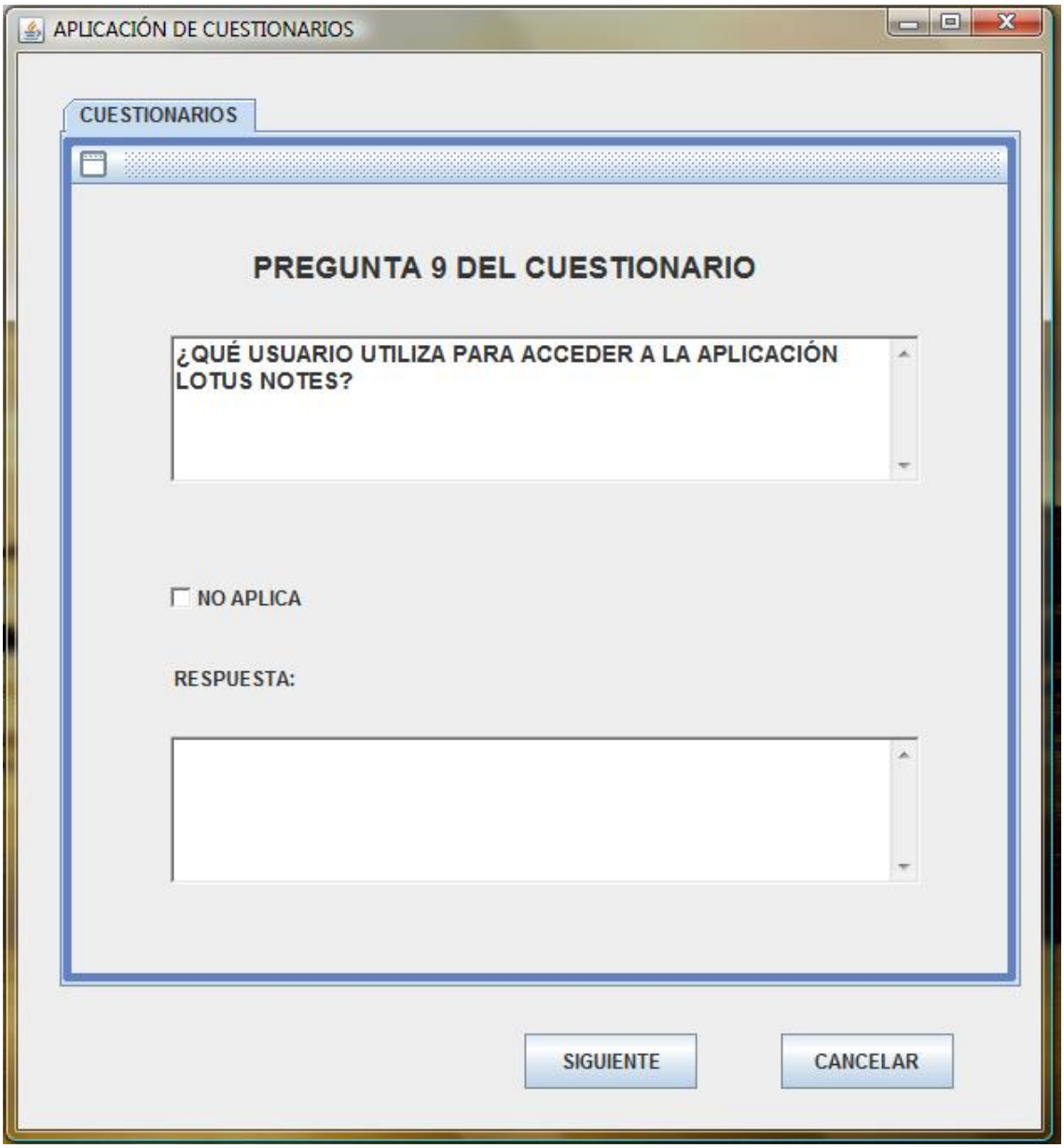

Figura 7.22: Pregunta 9 del cuestionario.

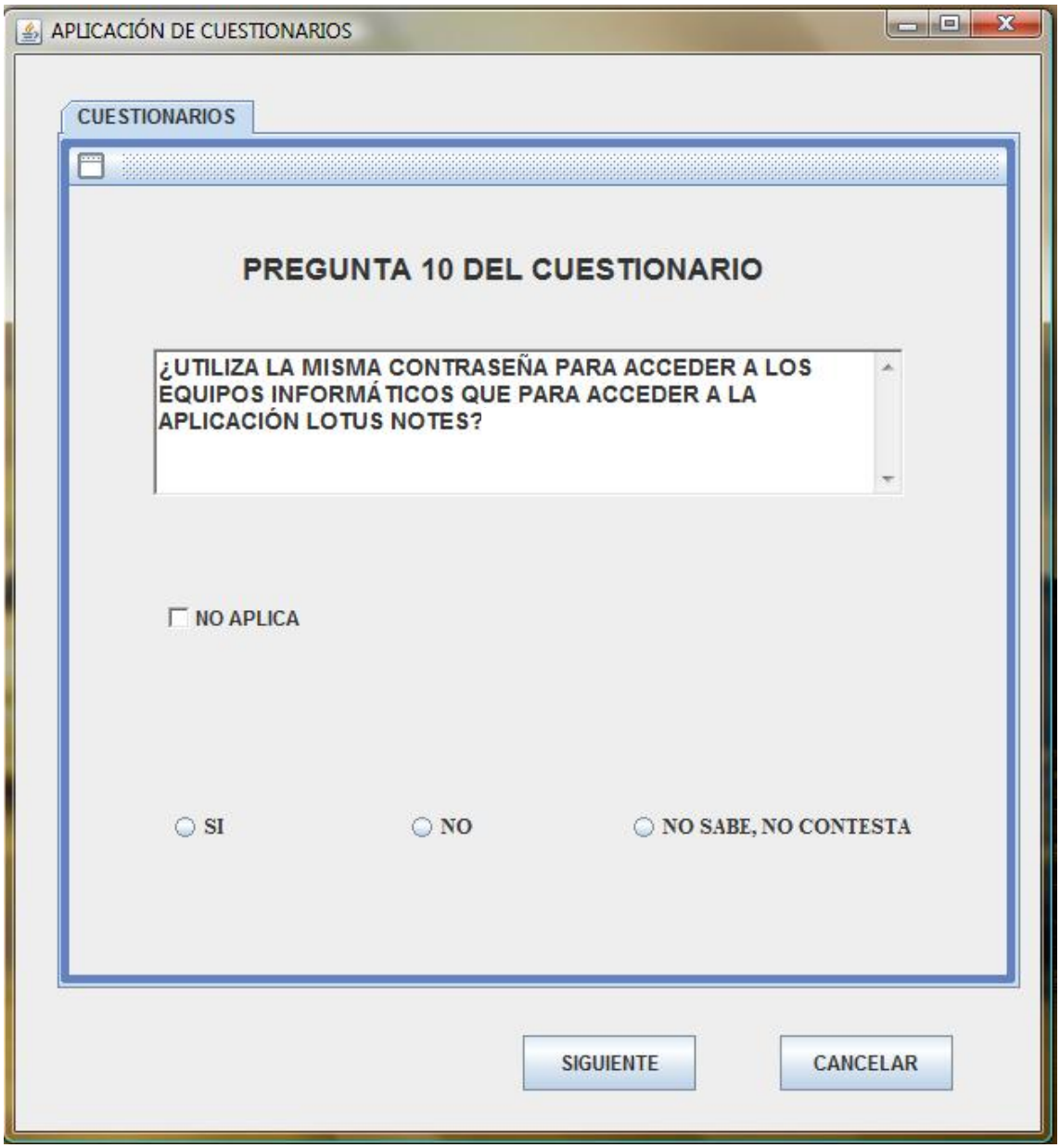

Figura 7.23: Pregunta 10 del cuestionario.

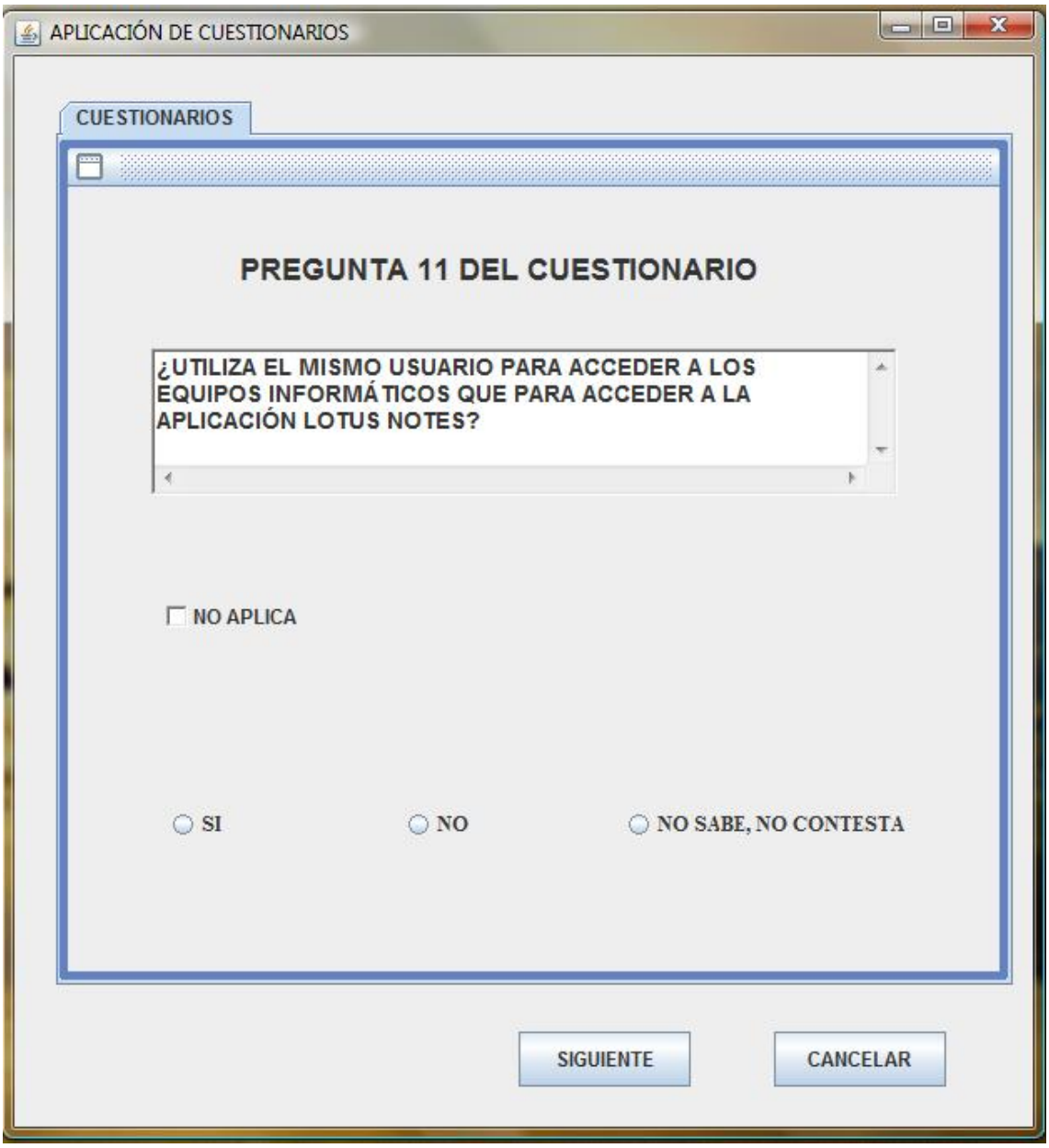

Figura 7.24: Pregunta 11 del cuestionario.

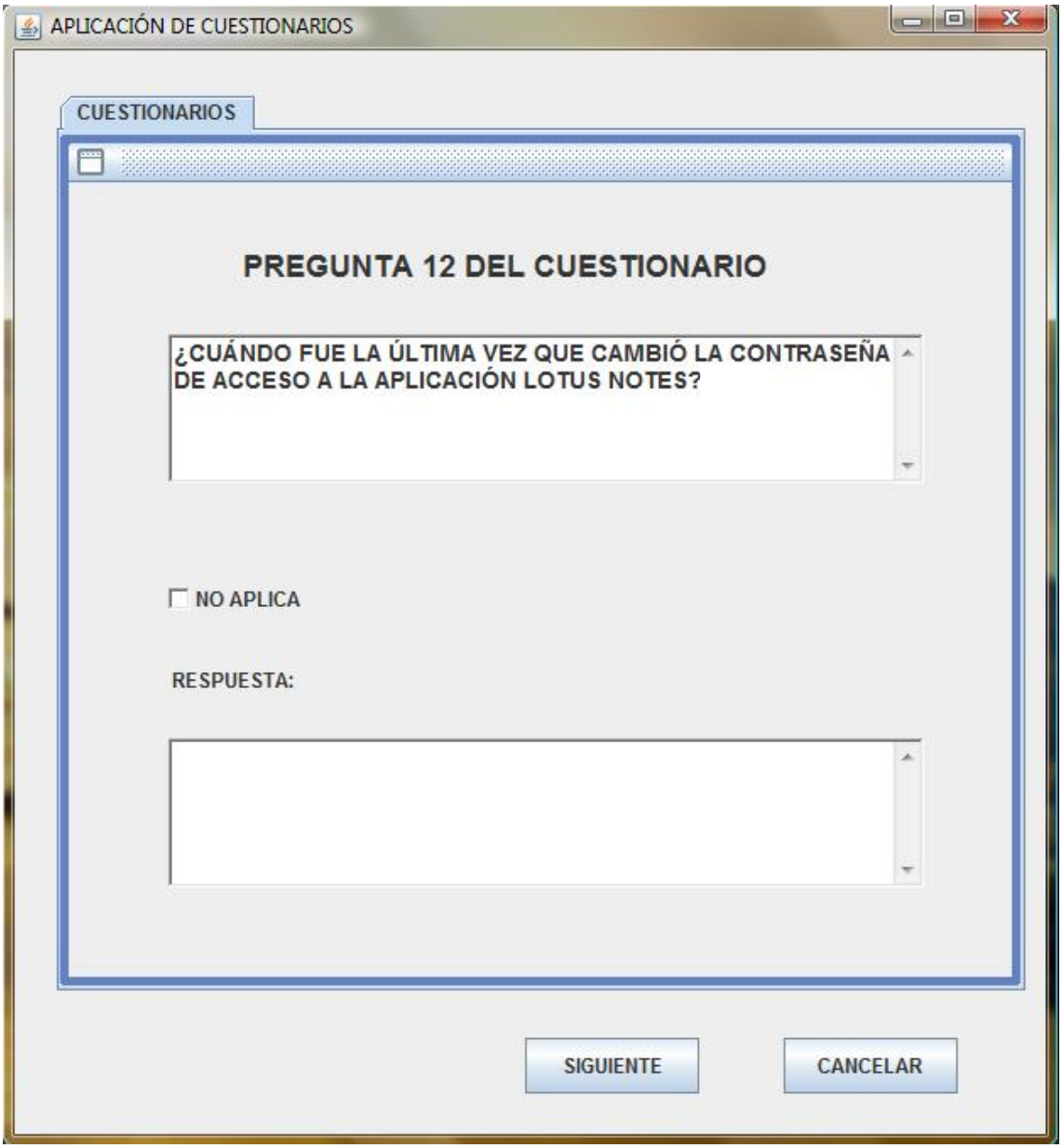

Figura 7.25: Pregunta 12 del cuestionario.

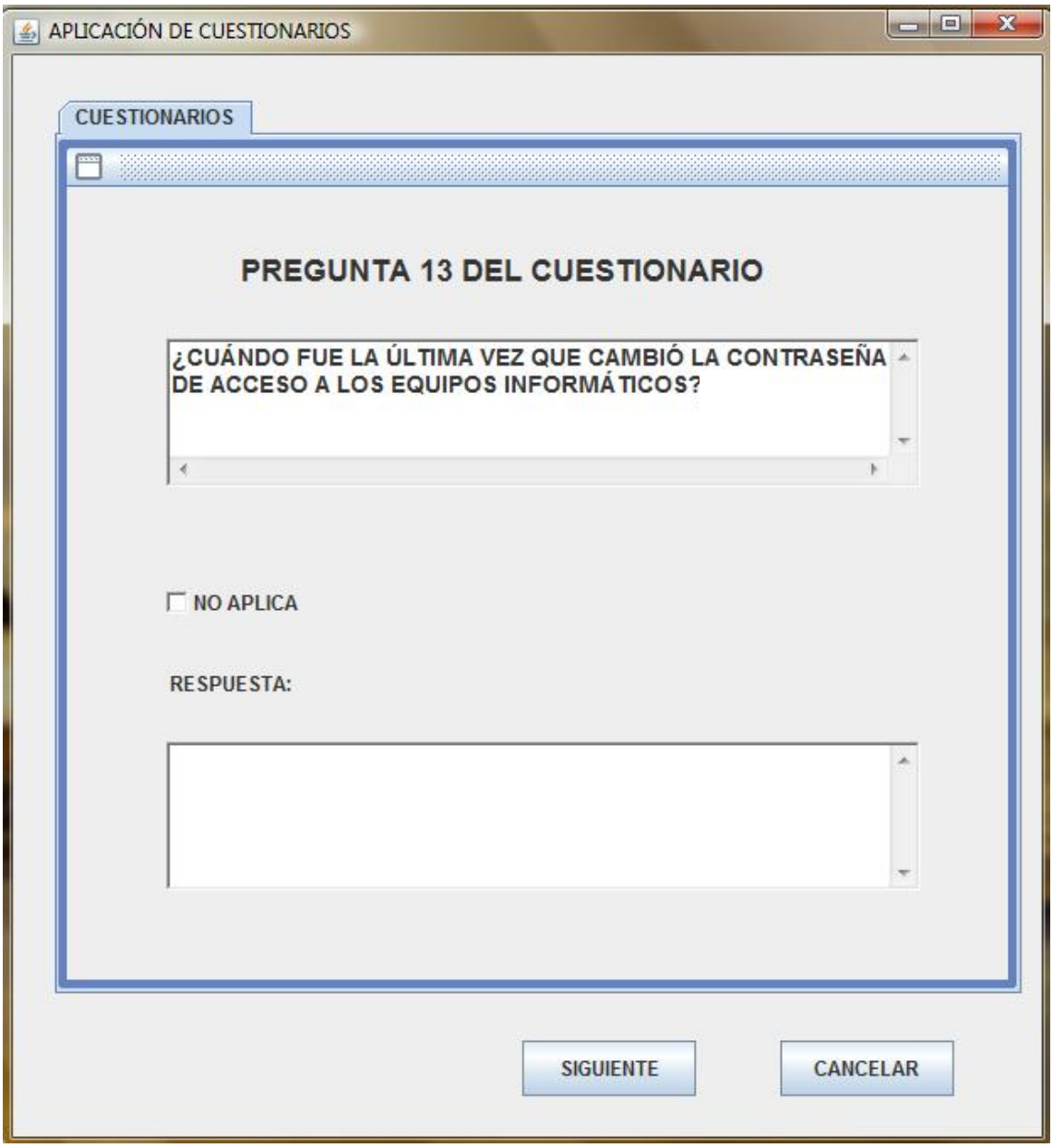

Figura 7.26: Pregunta 13 del cuestionario.

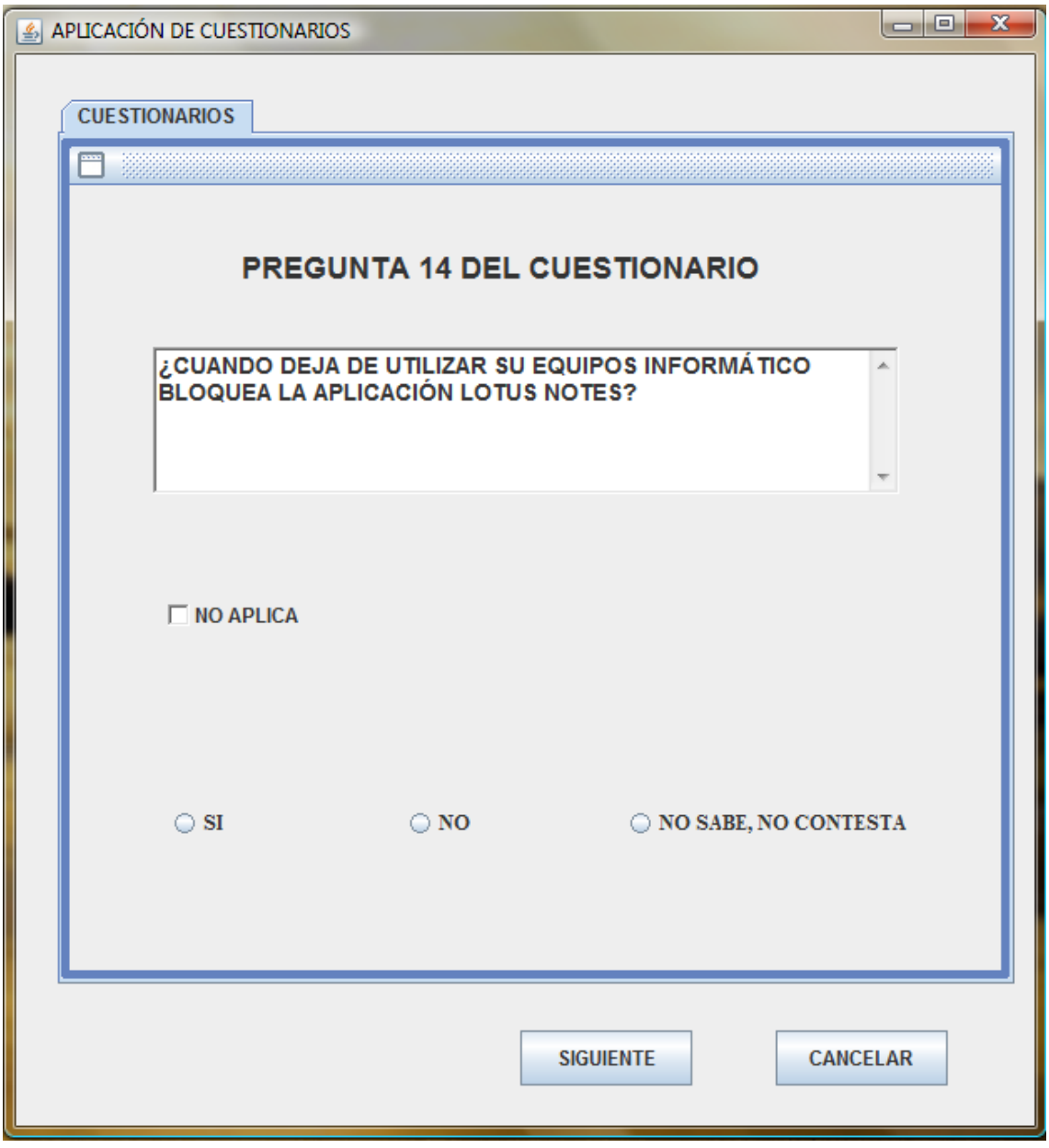

Figura 7.27: Pregunta 14 del cuestionario.

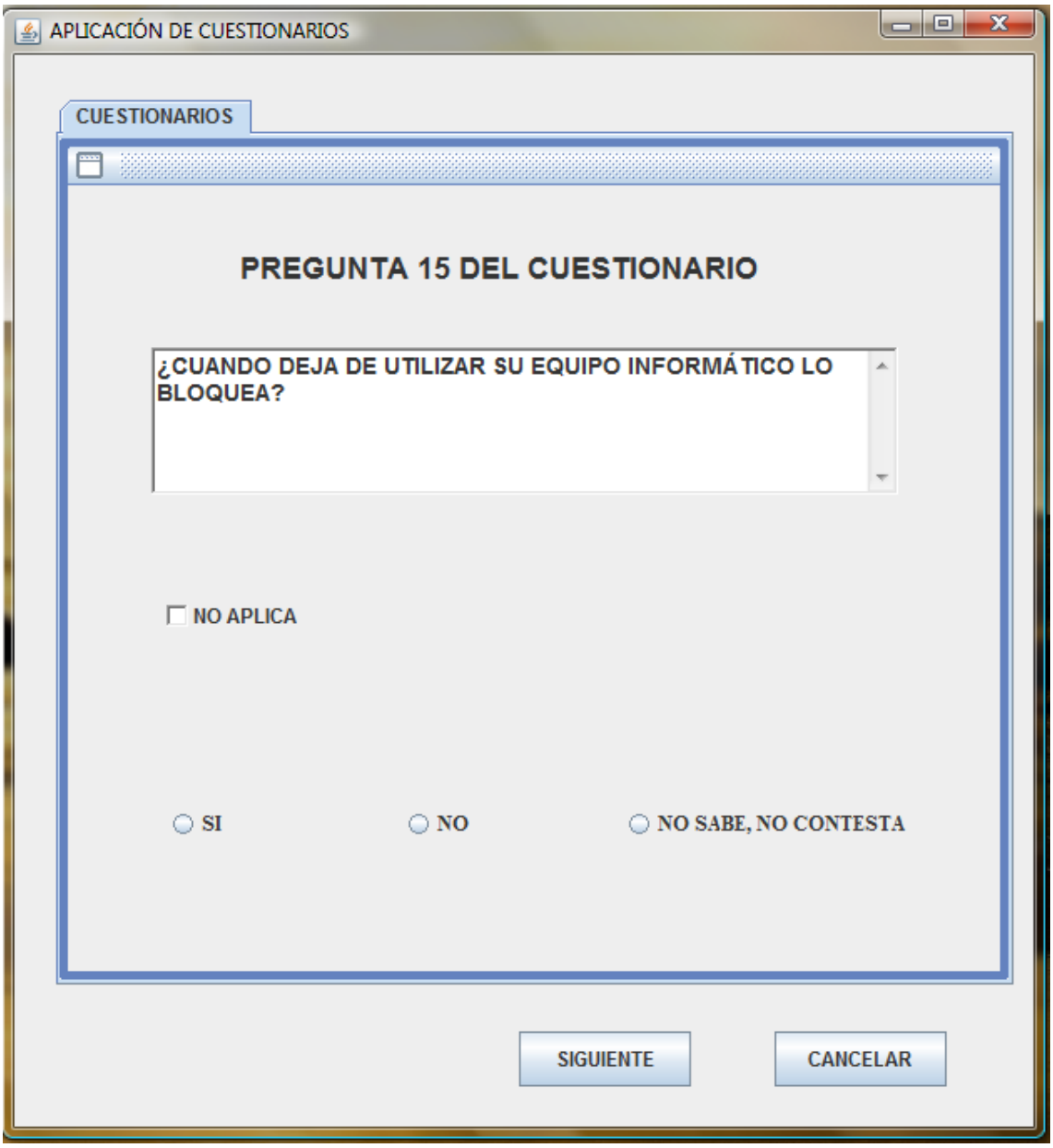

Figura 7.28: Pregunta 15 del cuestionario.

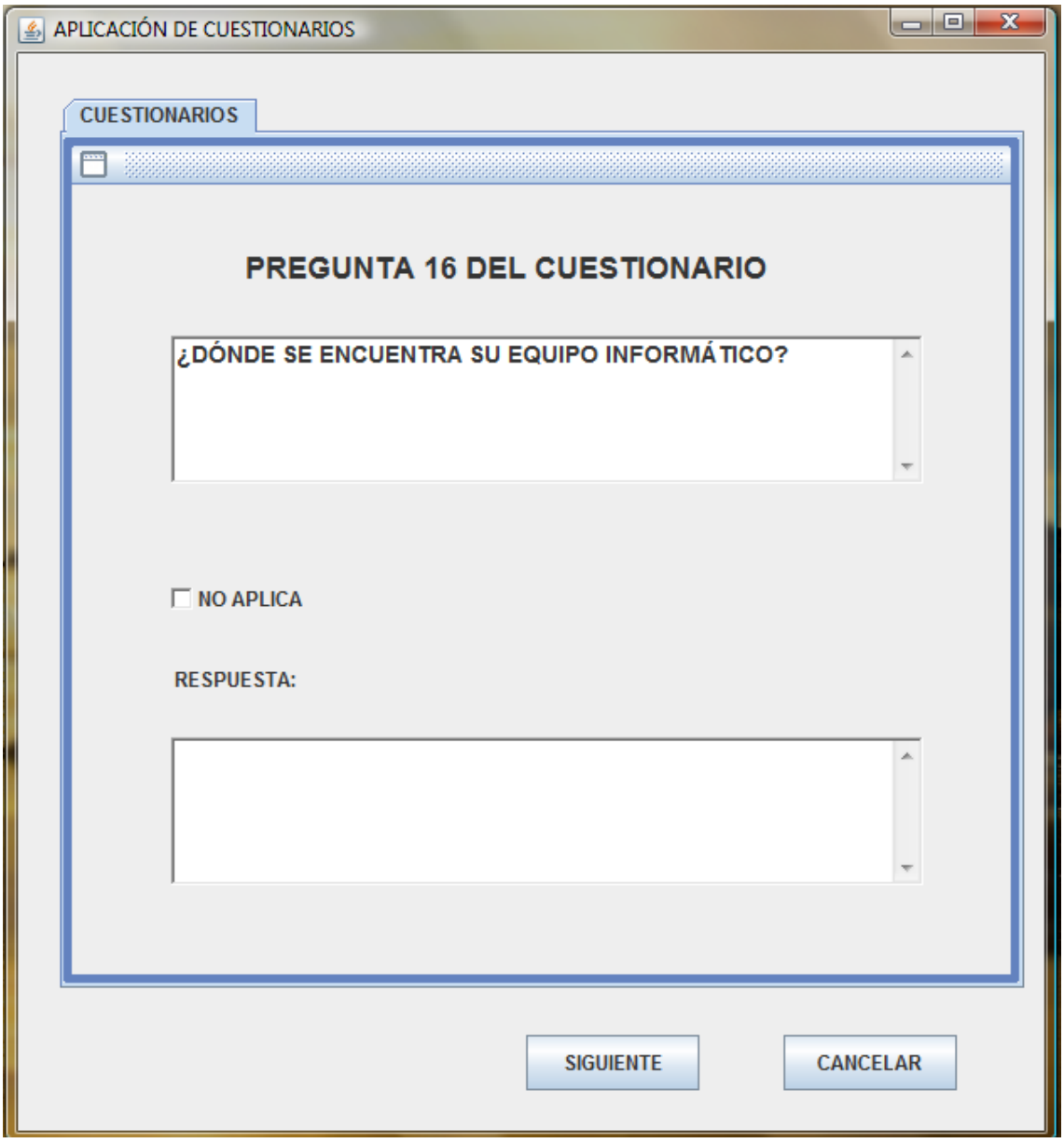

Figura 7.29: Pregunta 16 del cuestionario.

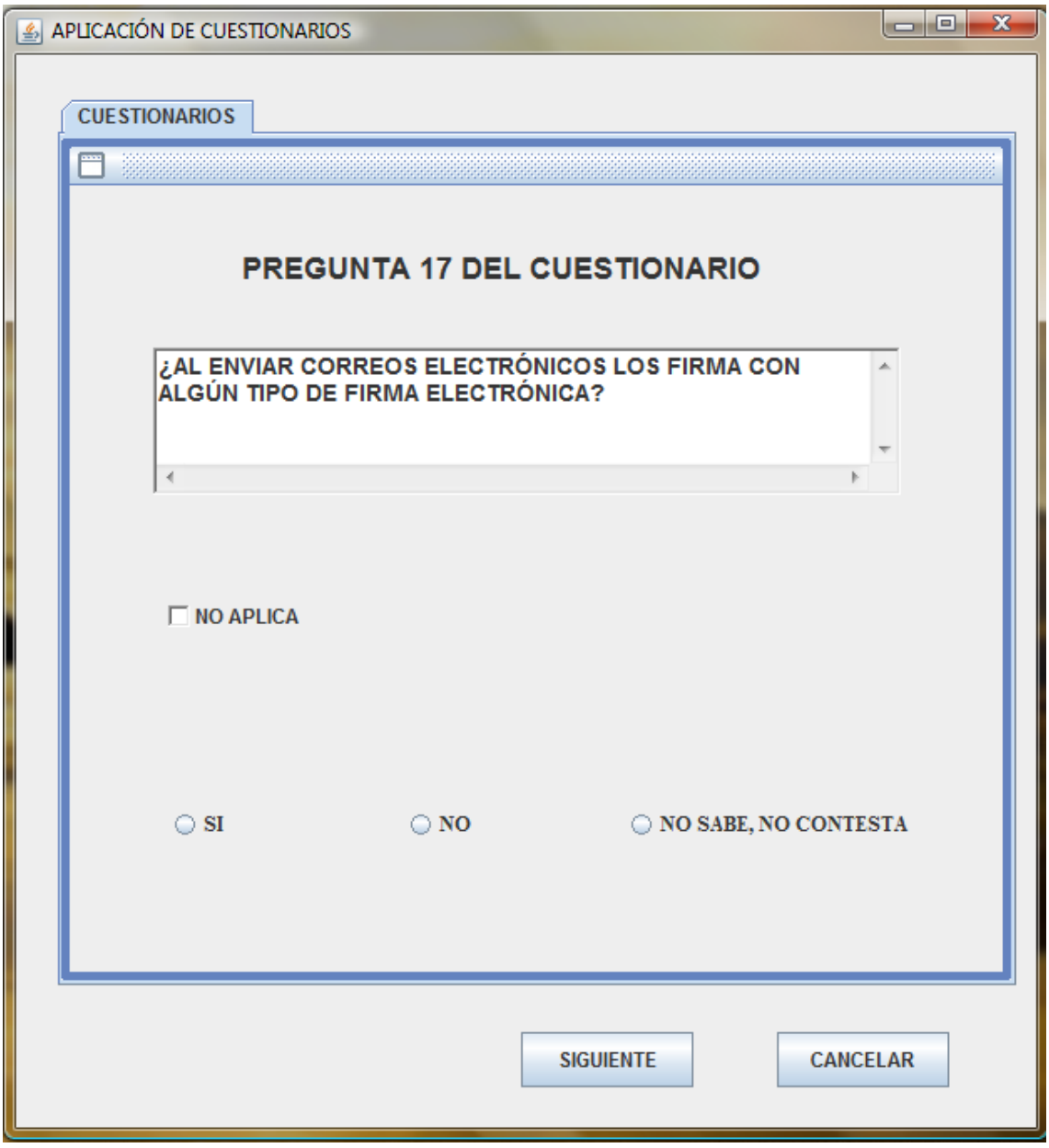

Figura 7.30: Pregunta 17 del cuestionario.

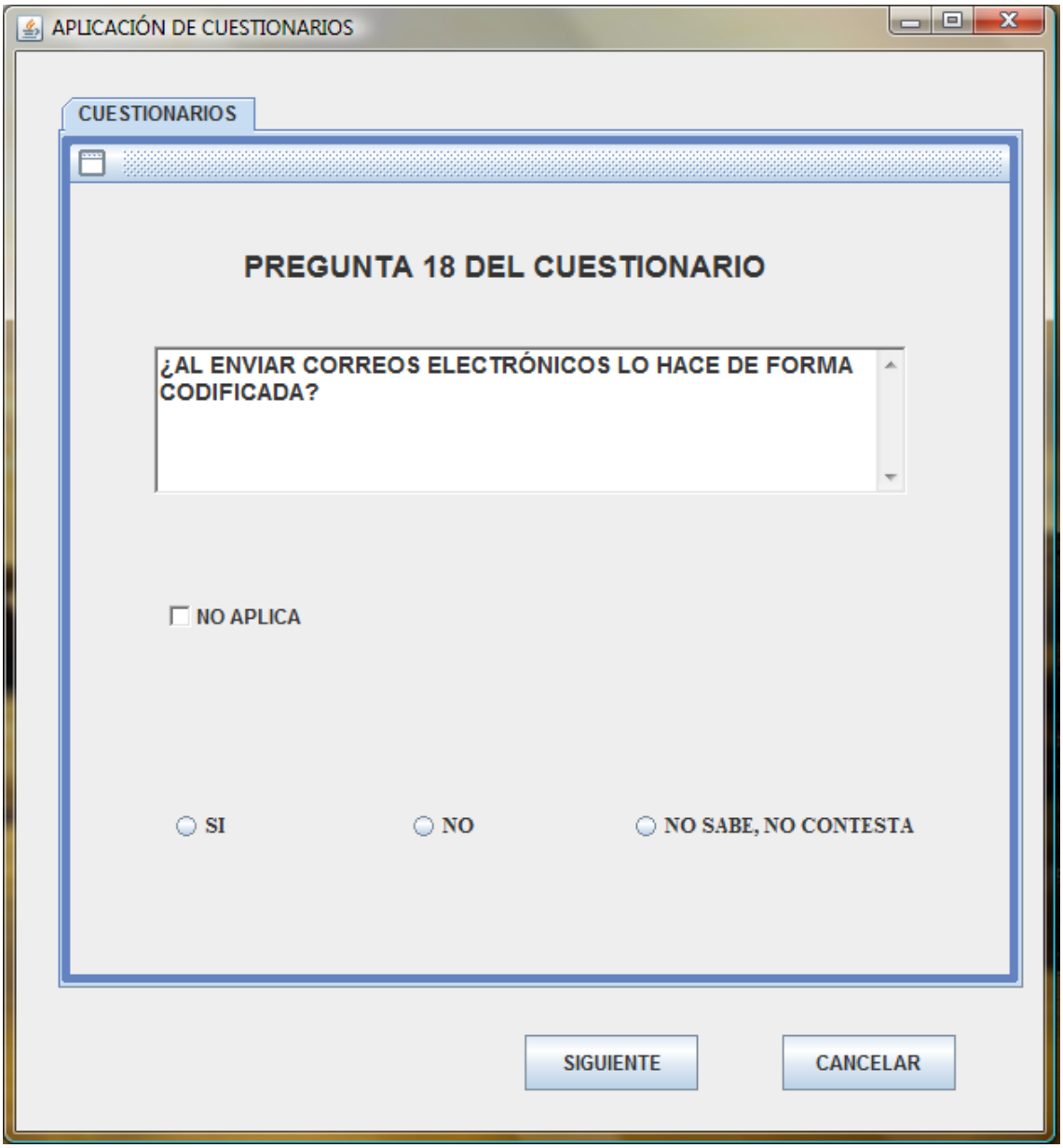

Figura 7.31: Pregunta 18 del cuestionario.

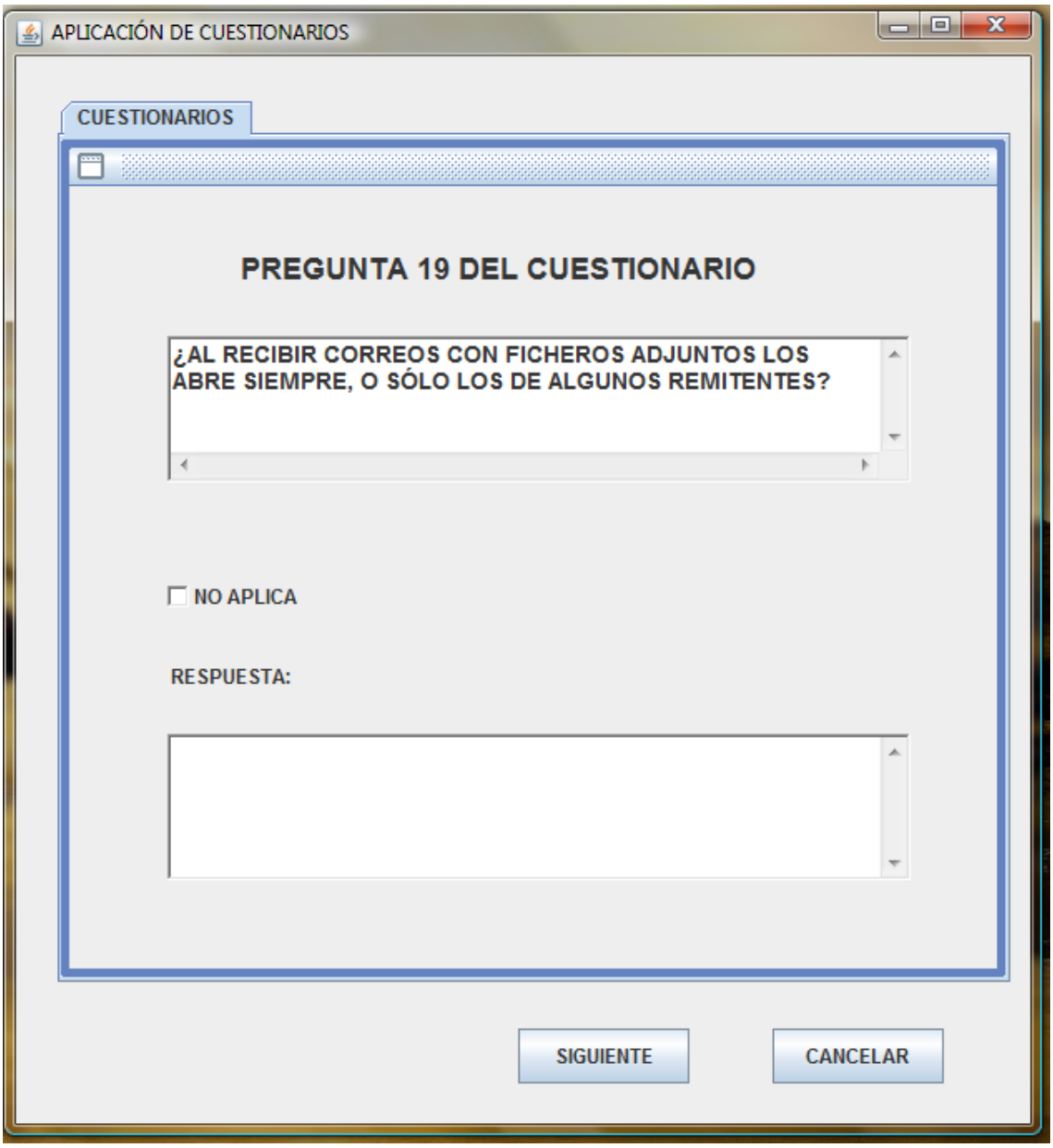

Figura 7.32: Pregunta 19 del cuestionario.

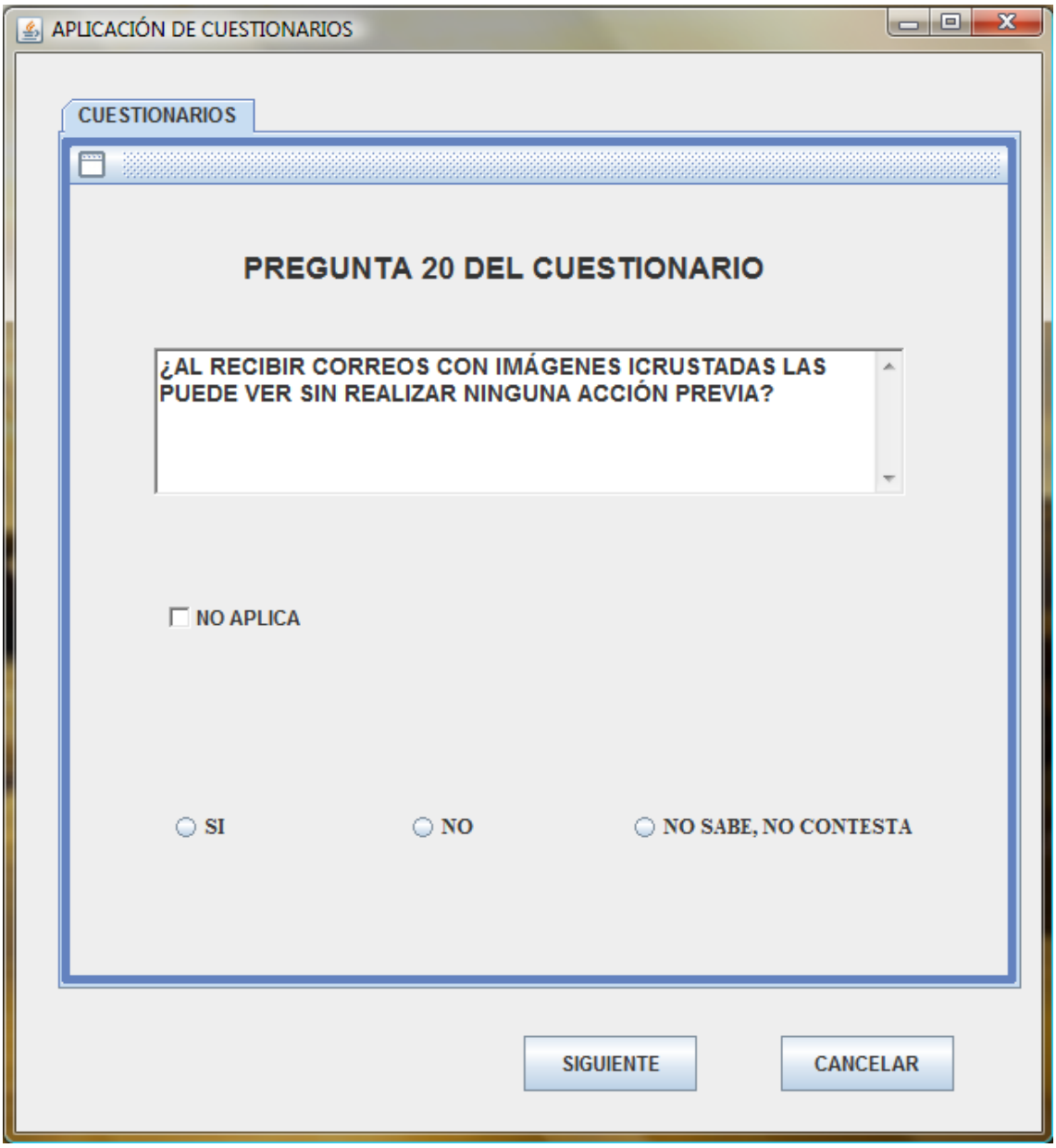

Figura 7.33: Pregunta 20 del cuestionario.

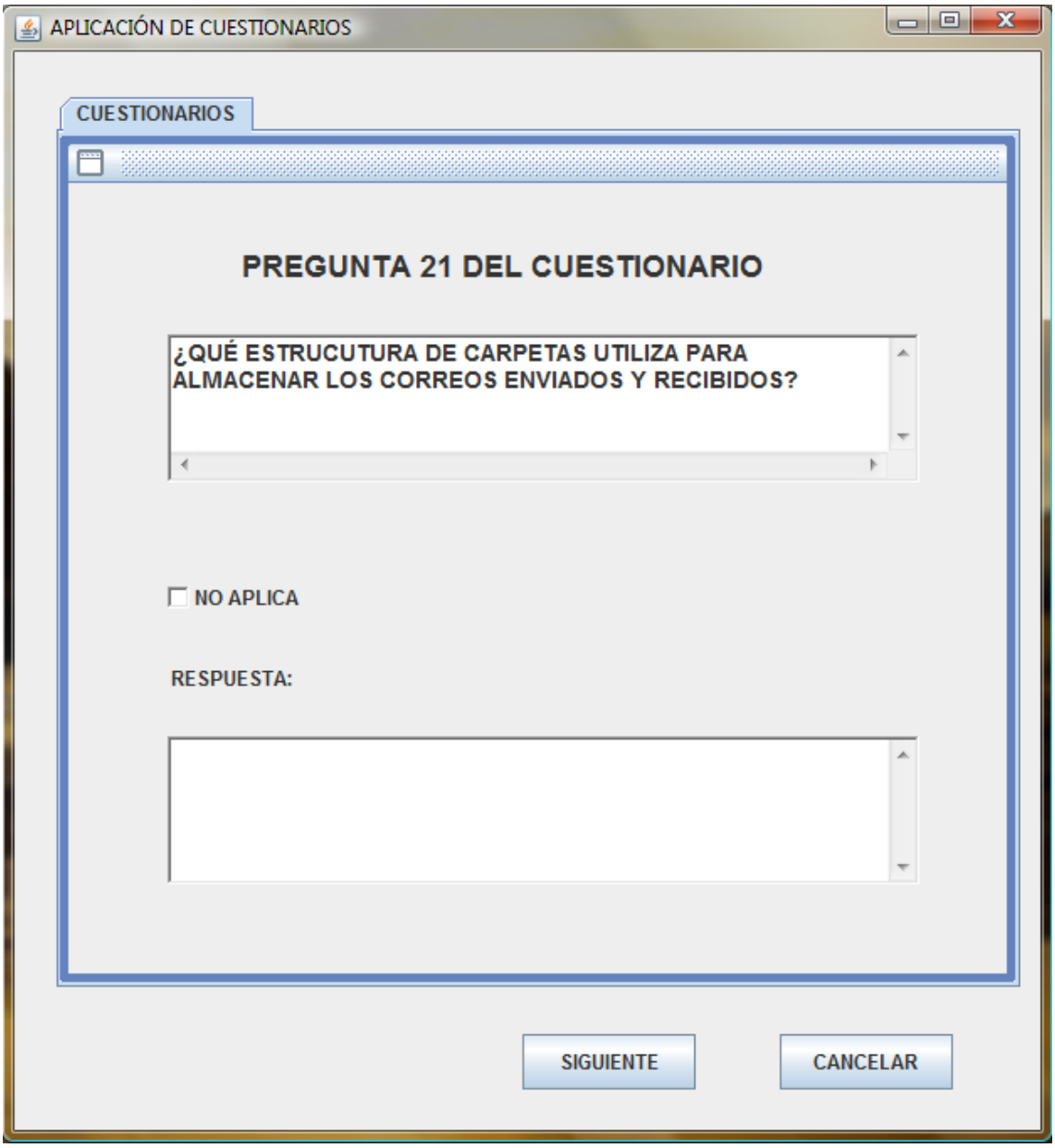

Figura 7.34: Pregunta 21 del cuestionario.

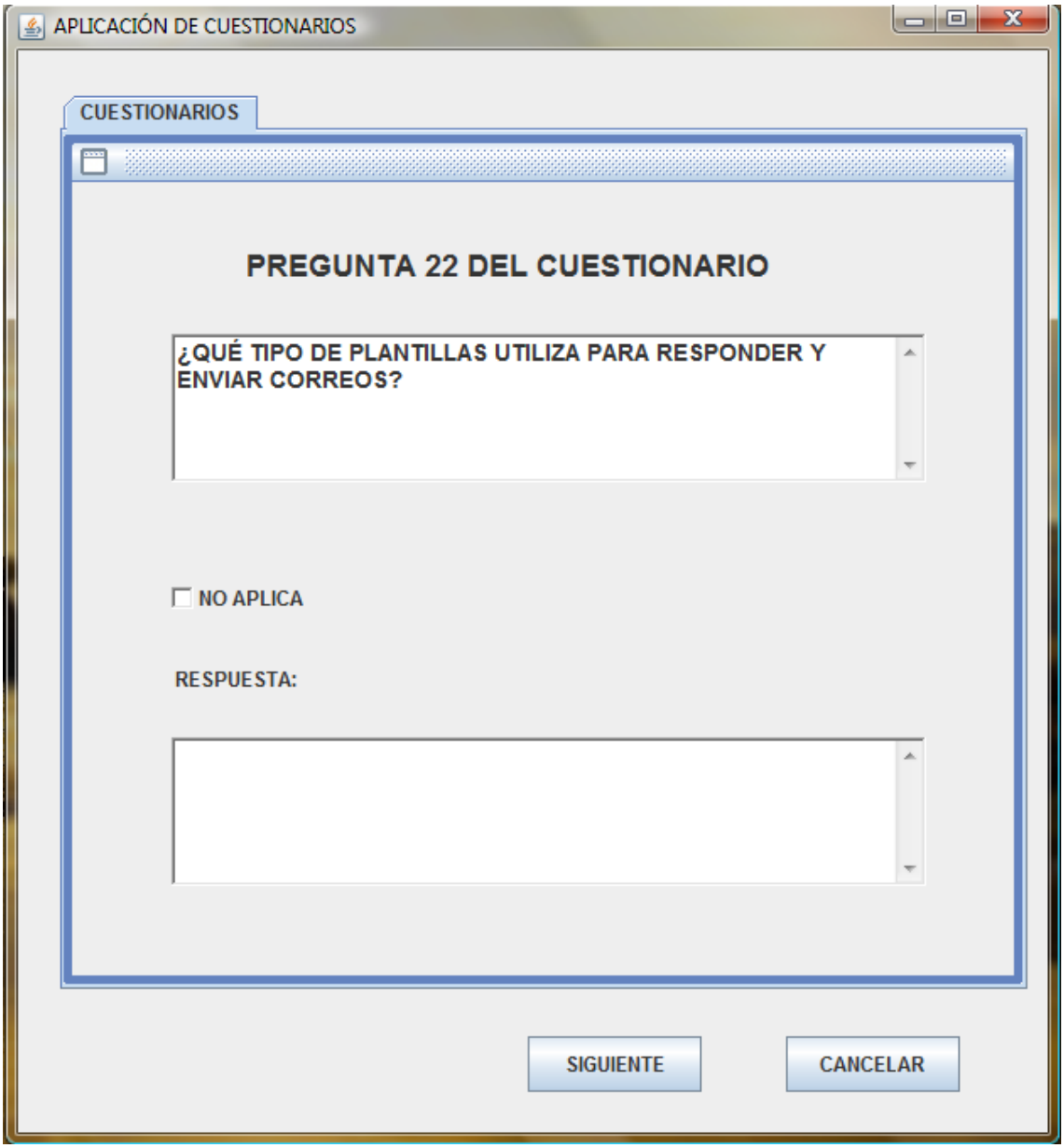

Figura 7.35: Pregunta 22 del cuestionario.

ANEXO A: ESTÁNDAR ISO 27002.

A lo largo de este anexo haremos un resumen del estándar ISO/IEC-27002 indicando cuales son los puntos más importantes del estándar, no sólo en relación al actual proyecto fin de carrera.

Hemos decidido incluirlo como anexo y no como apartado de la memoria, puesto que no hemos creído necesaria su inclusión, ya que únicamente es utilizado como una referencia más, pero no se sigue de forma exacta, aunque en el apartado dos del actual proyecto final de carrera mencionamos el estándar.

INTRODUCCIÓN.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

Se necesita establecer, implementar, controlar, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador, por

ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control de acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles.

La gestión de la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes u otros grupos externos. También se pueden requerir asesoría especializada de organizaciones externas.

Es esencial que una organización identifique sus requerimientos de seguridad.

Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio y su ambiente socio-cultural.

La última fuente es el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño comercial probable resultado de fallos en la seguridad.

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se debieran seleccionar los controles apropiados y se debieran implementar para asegurar que los riesgos se reduzcan a un nivel aceptable. La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales relevantes.

1. ALCANCE

Establece el lineamiento y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delimitados en este estándar internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Este estándar puede servir como lineamiento para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales.

2. TÉRMINOS Y DEFINICIONES.

A lo largo de este punto de el estándar se definen los siguientes términos: *activo, control, lineamiento, medios de procesamiento de la información, seguridad de la información, evento de seguridad de la información, incidente de seguridad de la información, política, riesgo, análisis del riesgo, evaluación del riesgo, gestión del riesgo, tratamiento del riesgo, tercera persona, amenaza y vulnerabilidad,* no hemos creído oportuno definir todos estos términos en este anexo, ya que es simplemente un resumen que debe servir a los lectores para hacerse una idea general del espíritu y ámbito de aplicación del estándar. Aunque alguno de los términos aparecerá definido en el glosario de términos, ya que es utilizado a lo largo de este anexo o de cualquier otro apartado del presente proyecto final de carrera.

3. ESTRUCTURA DEL ESTÁNDAR.

El estándar consta de 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

Cada cláusula contiene un número de categorías de seguridad principales. Las 11 cláusulas son:

- **Política de seguridad**
- **Organización de la seguridad de la información**
- **Gestión de activos**
- **Seguridad de recursos humanos**
- **Seguridad física y ambiental**
- **Gestión de comunicaciones y operaciones**
- **Control de acceso**
- **Adquisición, desarrollo y mantenimiento de sistemas de información**
- **Gestión de incidentes de seguridad de la información**
- **Gestión de la continuidad comercial**
- **Conformidad**.

4. EVALUACIÓN Y TRATAMIENTO DEL RIESGO.

Las evaluaciones del riesgo deberían identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización.

Los resultados debieran guiar y determinar la acción de gestión apropiada y las propiedades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar varias veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado.

5. POLÍTICA DE SEGURIDAD.

El objetivo es proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.

El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.

La política de seguridad de la información debiera ser revisada a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

6.1 Organización interna.

El objetivo es manejar la seguridad de la información dentro de la organización.

Se debiera establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

La gerencia debiera aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización.

Si fuese necesario, se debiera establecer una fuente de consultoría sobre seguridad de la información y debiera estar disponible dentro de la organización.

Se debieran desarrollar contactos con los especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias industriales, seguimiento de los estándares y evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información.

Se debiera fomentar un enfoque multidisciplinario para la seguridad de la información.

La gerencia debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.

Las actividades de la seguridad de la información debieran ser coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes.

Todas las responsabilidades de la seguridad de la información debieran estar claramente definidas.

Un proceso de la gerencia para la autorización de facilidades nuevas de procesamiento de información, debiera ser definido e implementado

Se debieran identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no divulgación reflejan las necesidades de la organización para proteger la información

Se debieran mantener los contactos apropiados con las autoridades relevantes.

Se debieran mantener contactos apropiados con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

Se debiera revisar el enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) de manera independiente a intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.

6.2 Grupos o personas externas.

El objetivo es mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.

La seguridad de la información y los medios de procesamiento de la información de la organización no debieran ser reducidos por la introducción de productos y servicios de grupos externos.

Se debiera controlar cualquier acceso a los medios de procesamiento de información de la organización y el procesamiento y comunicación de la información realizado por grupos externos.

Cuando existe la necesidad comercial de trabajar con grupos externos que pueden requerir acceso a la información y a los medios de procesamiento de información de la organización, u obtener o proveer un producto y servicio de o a un grupo externo, se debiera llevar a cabo una evaluación del riesgo para determinar las implicaciones en la seguridad y los requerimientos de control. Se debieran acordar y definir los controles en un acuerdo con el grupo externo.

Se debieran identificar los riesgos para la información y los medios de procesamiento de la información de la organización a raíz de procesos comerciales que involucran a grupos externos y se debieran implementar controles apropiados antes de otorgarles acceso.

Se debieran tratar todos los requerimientos de seguridad identificados antes de proporcionar a los clientes acceso a la información o activos de la organización.

Los acuerdos o contratos con terceros que involucran el acceso, procesamiento, comunicación o manejo de la información o medios de procesamiento de información de la compañía, o agregan productos o servicios a los medios de procesamiento de información debieran abarcar todos los requerimientos de seguridad relevantes.

7. GESTIÓN DE ARCHIVOS.

7.1 Responsabilidad de los activos.

El objetivo es lograr y mantener una apropiada protección de los activos organizacionales.

Todos los activos debieran ser inventariados y contar con un propietario nombrado.

Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

7.2 Clasificación de la información.

El objetivo es asegurar que la información reciba un nivel de protección apropiado.

La información debiera ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial.

Se debiera utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

8 SEGURIDAD DE RECURSOS HUMANOS.

8.1 Antes del empleo.

El objetivo es asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad debieran ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo.

Los antecedentes de todos los candidatos al empleo, contratistas y terceros debieran ser adecuadamente investigados, especialmente para los trabajos confidenciales.

Los empleados, contratistas y terceros usuarios de los medios de procesamiento de la información debieran firmar un acuerdo sobre sus roles y responsabilidades con relación a la seguridad.

8.2 Durante el empleo.

El objetivo es asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se debieran definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro de la organización.

Se debiera proporcionar a todos los usuarios empleados, contratistas y terceras personas un nivel adecuado de conocimiento, educación y capacitación en procedimientos de seguridad y uso correcto de los medios de procesamiento de información para minimizar los posibles riesgos de seguridad. Se debiera establecer un proceso disciplinario normal para manejar los fallos en la seguridad.

8.3 Terminación o cambio de empleo.

El objetivo es asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada.

Se debieran establecer las responsabilidades para asegurar que la salida de la organización del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

Los cambios en las responsabilidades y empleos dentro de la organización se pueden manejar como la terminación de la responsabilidad o empleo respectivo en concordancia con esta sección, y cualquier empleo nuevo debiera ser manejado tal como se describe en la sección 8.1.

9. SEGURIDAD FÍSICA Y AMBIENTAL.

9.1 Áreas seguras.

El objetivo es evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

Se debiera diseñar y aplicar la seguridad física para las oficinas, habitaciones y medios.

Se debiera asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se debiera diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas.

Se debieran controlar los puntos de acceso como las áreas de entrega y carga y otros puntos por donde personas no autorizadas puedan ingresar al local y, si fuese posible, debieran aislarse de los medios de procesamiento de información para evitar el acceso no autorizado.

9.2 Equipo de seguridad.

El objetivo es evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

Se debiera proteger el equipo de amenazas físicas y ambientales.

La protección del equipo (incluyendo aquel utilizado fuera del local y la eliminación de propiedad) es necesaria para reducir el riesgo de acceso no-autorizado a la información y proteger contra pérdida o daño. Esto también debiera considerar la ubicación y eliminación del equipo. Se pueden requerir controles especiales para proteger el equipo contra amenazas físicas, y salvaguardar los medios de soporte como el suministro eléctrico y la infraestructura del cableado.

Se debiera ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no autorizado.

Se debiera proteger el equipo de fallos de energía y otras interrupciones causadas por fallos en los servicios públicos de soporte

El cableado de la energía y las telecomunicaciones que llevan los datos o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño.

Se debiera mantener correctamente el equipo para asegurar su continua disponibilidad e Integridad

Se debiera aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.

Se debieran revisar los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier dato confidencial o licencia de software antes de su eliminación

El equipo, información o software no debiera retirarse sin autorización previa.

10. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES.

10.1 Procedimientos y responsabilidades operacionales.

El objetivo es asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se debieran establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.

Cuando sea apropiado, se debiera implementar la segregación de deberes para reducir el riesgo de negligencia o mal uso deliberado del sistema.

10.2 Gestión de la entrega de servicios de terceros.

El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.

La organización debiera chequear la implementación de los acuerdos, verificar su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

10.3 Planeación y aceptación del sistema.

El objetivo es minimizar el riesgo de fallos en el sistema.

Se requiere de planeación y preparación anticipadas para asegurar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño del sistema requerido.

Se debieran realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema.

Se debieran establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso.

10.4 Protección contra el código masivo y móvil.

El objetivo es proteger la integridad del software y la integración.

Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como virus cómputo, virus de red, caballos Troyanos y bombas lógicas. Los usuarios debieran estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes debieran introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

10.5 Respaldo o back-up.

El objetivo es mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Se debieran establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver también 14.1) para tomar copias de respaldo de los datos y practicar su restauración oportuna

10.6 Gestión de seguridad de la red.

El objetivo es asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, seguimiento y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

10.7 Gestión de medios.

El objetivo es evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales.

Los medios se debieran controlar y proteger físicamente.

Se debieran establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), input/output de datos y documentación del sistema de una divulgación no-autorizada, modificación, eliminación destrucción.

10.8 Intercambio de información.

El objetivo es mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.

Los intercambios de información y software dentro de las organizaciones se debieran basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante (cláusula 15).

Se debieran establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en-tránsito.

10.9 Servicios de comercio electrónico.

El objetivo es asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.

Se debieran considerar las implicancias de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo las transacciones en-línea, y los requerimientos de controles. También se debieran considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de los sistemas públicamente disponibles

10.10 Monitorización.

El objetivo es detectar las actividades de procesamiento de información no autorizadas.

Se debieran monitorizar los sistemas y se debieran reportar los eventos de seguridad de la información. Se debieran utilizar bitácoras de operador y se debieran registrar las fallos para asegurar que se identifiquen los problemas en los sistemas de información.

Una organización debiera cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitorización y registro.

Se debiera utilizar la monitorización del sistema para chequear la efectividad de los controles adoptados y para verificar la conformidad con un modelo de política de acceso.

11. CONTROL DE ACCESO.

11.1 Requerimiento del negocio para el control de acceso.

El objetivo es controlar el acceso a la información.

Se debiera controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.

Las reglas de control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información.

Se debiera establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.

11.2 Gestión de acceso del usuario.

El objetivo es asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información

Se debieran establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la eliminación del registro final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debiera prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema.

Debiera existir un procedimiento formal para el registro y eliminación del registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información.

Se debiera restringir y controlar la asignación y uso de privilegios.

La asignación de claves secretas se debiera controlar a través de un proceso de gestión formal.

La gerencia debiera revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.

11.3 Responsabilidades del usuario.

El objetivo es evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios debieran estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

Se debiera implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y medios de procesamiento de la información.

Se debiera requerir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de claves secretas.

Los usuarios debieran asegurar que el equipo desatendido tenga la protección apropiada.

Se debiera adoptar una política de escritorio limpio para papeles y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.

11.4 Control de acceso a la red.

El objetivo es evitar el acceso no autorizado a los servicios de la red.

Se debiera controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no debieran comprometer la seguridad de los servicios de la red asegurando:

a) que existan las interfaces apropiadas entre la red de la organización y las redes de otras organizaciones, y redes públicas;

b) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;

c) el control del acceso del usuario a la información sea obligatorio.

Los usuarios sólo debieran tener acceso a los servicios para los cuales hayan sido específicamente autorizados.

Se debieran utilizar métodos de autenticación apropiados para controlar el acceso de usuarios remotos.

La identificación automática del equipo se debiera considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos

11.5 Control de acceso al sistema operativo.

El objetivo es evitar el acceso no autorizado a los sistemas operativos.

Se debieran utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados. Los medios debieran tener la capacidad para:

a) autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida;

b) registrar los intentos exitosos y fallidos de autenticación del sistema;

c) registrar el uso de los privilegios especiales del sistema;

d) emitir alarmas cuando se violan las políticas de seguridad del sistema;

e) proporcionar los medios de autenticación apropiados;

f) cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

El acceso a los sistemas operativos debiera ser controlado mediante un procedimiento de registro seguro.

Todos los usuarios tienen un identificador único (ID de usuario) para su uso personal, y se debiera escoger una técnica de autenticación adecuada para sustanciar la identidad de un usuario.

Los sistemas para el manejo de claves secretas debieran ser interactivos y debieran asegurar claves secretas adecuadas.

Se debiera restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación.

Las sesiones inactivas debieran ser cerradas después de un período de inactividad definido.

Se debieran utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional para las aplicaciones de alto riesgo.

11.6 Control de acceso a la aplicación y la información.

El objetivo es evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

Se debieran utilizar medios de seguridad para restringir el acceso a y dentro de los sistemas de aplicación.

El acceso lógico al software de la aplicación y la información se debiera limitar a los usuarios autorizados. Los sistemas de aplicación debieran:

a) controlar el acceso del usuario a la información y las funciones del sistema de aplicación, en concordancia con una política de control de acceso definida;

b) proporcionar protección contra un acceso no autorizado de cualquier utilidad, software del sistema de operación y software malicioso que sea capaz de superar o pasar los controles del sistema o la aplicación;

c) no comprometer a otros sistemas con los cuales se comparten recursos de información.

El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema.

Los sistemas confidenciales debieran tener un ambiente de cómputo dedicado (aislado).

11.7 Computación y teletrabajo móvil.

El objetivo es asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles.

La protección requerida se debiera conmensurar con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se debieran considerar los riesgos de trabajar en un ambiente desprotegido y se

debiera aplicar la protección apropiada. En el caso del teletrabajo, la organización debiera aplicar protección al lugar del teletrabajo y asegurar que se establezcan los arreglos adecuados para esta manera de trabajar.

Se debiera establecer una política y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil.

Se debiera desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

12.1 Requerimientos de seguridad de los sistemas de información.

El objetivo es garantizar que la seguridad sea una parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones comerciales, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso comercial puede ser crucial para la seguridad. Se debieran identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

12.2 Procesamiento correcto a las aplicaciones.

El objetivo es prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.

Se debieran diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para asegurar un procesamiento correcto. Estos controles debieran incluir la validación del input de datos, procesamiento interno y output de datos.

Se pueden requerir controles adicionales para los sistemas que procesan, o tienen impacto sobre, la información confidencial, valiosa o crítica. Estos

controles se debieran determinar sobre la base de los requerimientos de seguridad y la evaluación del riesgo.

12.3 Controles criptográficos.

El objetivo es proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos. Se debiera desarrollar una política sobre el uso de controles criptográficos. Se debiera establecer una gestión clave para sostener el uso de técnicas criptográficas.

12.4 Seguridad de los archivos del sistema.

El objetivo es garantizar la seguridad de los archivos del sistema.

Se debiera controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos de tecnología e investigación y las actividades de soporte se debieran realizar de una manera segura.

12.5 Seguridad en los procesos de desarrollo y soporte.

El objetivo es mantener la seguridad del software y la información del sistema de aplicación.

Se debiera controlar estrictamente los ambientes del proyecto y soporte.

Los gerentes responsables por los sistemas de aplicación también debieran ser responsables por la seguridad del ambiente del proyecto o el soporte. Ellos debieran asegurar que todos los cambios propuestos para el sistema sean revisados para revisar que no comprometan la seguridad del sistema o el ambiente de operación.

12.6 Gestión de la vulnerabilidad técnica.

El objetivo es reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

Se debiera implementar una gestión de la vulnerabilidad técnica de una manera efectiva, sistemática y respetable, tomando mediciones para confirmar su efectividad. Estas consideraciones debieran incluir a los sistemas de operación, y cualquier otra aplicación en uso.

13. GESTIÓN DE UN INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Reporte de los eventos y debilidades de la seguridad de la información.

El objetivo es asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

Se debieran establecer procedimientos formales de reporte y de la intensificación de un evento. Todos los usuarios empleados contratistas y terceros debieran estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales. Se les debiera requerir que reporten cualquier evento y debilidad de la seguridad de la información lo más rápidamente posible en el punto de contacto designado.

Los eventos de seguridad de la información debieran ser reportados a través de los canales gerenciales apropiados lo más rápidamente posible.

Se debiera requerir que todos los usuarios empleados, contratistas y terceros de los sistemas y servicios de información tomen nota de y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios

13.2 Gestión de los incidentes y mejoras en la seguridad de la información.

El objetivo es asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

Se debieran establecer las responsabilidades y procedimientos para manejar de manera efectivo los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debiera aplicar un proceso de mejoramiento continuo para la respuesta a, monitorización, evaluación y la gestión general de los incidentes en la seguridad de la información.

Cuando se requiera evidencia, esta se debiera recolectar cumpliendo con los requerimientos legales.

Se debieran establecer las responsabilidades y los procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la información

Se debieran establecer mecanismos para permitir cuantificar y monitorizar los tipos, volúmenes y costos de los incidentes en la seguridad de la información

Cuando una acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (ya sea civil o criminal); se debiera recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s).

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio.

El objetivo es contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallos importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Se debiera implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la organización y recuperarse de la pérdidas de activos de información (lo cual puede ser resultado de, por ejemplo, desastres naturales, accidentes, fallos del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación. Este proceso debiera identificar los procesos comerciales críticos e integrar los requerimientos de gestión de la seguridad de la información de la continuidad del negocio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y medios.

Las consecuencias de los desastres, fallos en la seguridad, pérdida del servicio y la disponibilidad del servicio debieran estar sujetas a un análisis del impacto comercial. Se debieran desarrollar e implementar planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales. La seguridad de la información debiera ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización.

La gestión de la continuidad del negocio debiera incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debiera limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos comerciales.

Se debiera desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización

Se debieran identificar los eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

Se debieran desarrollar e implementar planes para mantener restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o fallo, de los procesos comerciales críticos.

Se debiera mantener un solo marco referencial de los planes de continuidad del negocio para asegurar que todos los planes sean consistentes, tratar consistentemente los requerimientos de seguridad de la información e identificar las prioridades para la prueba y el mantenimiento.

Los planes de continuidad del negocio debieran ser probados y actualizados regularmente para asegurar que sean actuales y efectivos

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requerimientos legales.

El objetivo es evitar las violaciones de cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

Se debiera buscar la asesoría sobre los requerimientos legales específicos de los asesores legales de la organización o profesionales legales calificados adecuados. Los requerimientos legislativos varían de un país a otro y pueden variar para la información creada en un país que es transmitida a otro país (es decir, flujo de datos inter-fronteras).

Se debiera definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes, y el enfoque de la organización para satisfacer esos requerimientos, para cada sistema de información y la organización.

Se debieran implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso del material con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado.

Se debieran proteger los registros importantes de pérdida, destrucción, falsificación; en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

Se debiera asegurar la protección y privacidad de los datos conforme lo requiera la legislación, regulaciones y, si fuesen aplicables, las cláusulas contractuales relevantes.

Se debiera disuadir a los usuarios de utilizar los medios de procesamiento de la información para propósitos no autorizados.

Los controles criptográficos se debieran utilizar en cumplimiento con todos los acuerdos, leyes y regulaciones relevantes.

15.2 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico.

El objetivo es asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

La seguridad de los sistemas de información se debiera revisar regularmente.

Estas revisiones debieran realizarse en base a las políticas de seguridad apropiadas y las plataformas técnicas, y los sistemas de información debieran ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.

Los gerentes debieran asegurar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para asegurar el cumplimiento de las políticas y estándares de seguridad.

Los sistemas de información debieran verificarse regularmente para ver el cumplimiento de los estándares de implementación de la seguridad.

15.3 Consideraciones de auditoría de los sistemas de información.

El objetivo es maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoría.

Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas operacionales debieran ser planeados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos comerciales.

Se debiera proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o trasgresión posible.

ANEXO B: INSTALACIÓN LOTUS NOTES.

A lo largo de este anexo haremos un breve resumen gráfico y explicativo de cómo se puede instalar la aplicación Lotus Notes en un ordenador personal.

No explicaremos cómo conseguir la aplicación Lotus Notes, puesto que nosotros sólo hemos trabajado con una versión de evaluación descargada desde la página oficial de IBM, aunque es posible comprar la aplicación vía on-line desde la página oficial de IBM.

Únicamente explicaremos qué pasos se deben seguir para realizar la instalación básica, no explicaremos qué pasos se deben seguir para realizar una instalación segura, ya que en el apartado 5 del actual proyecto fin de carrera hemos explicado cuál debe ser la configuración correcta de la aplicación Lotus Notes desde el punto de vista de la seguridad, por lo tanto no hemos creído necesario volver a repetir en este anexo qué puntos de la configuración modificar y qué valores deben tener.

Durante la instalación indicaremos qué ventajas e inconvenientes tienen las distintas opciones de instalación, qué complementos se instalan con las diferentes opciones de instalación y qué funcionalidades tienen los distintos complementos de la instalación de Lotus Notes.

A continuación procedemos a detallar el proceso de instalación de la aplicación Lotus Notes.

Tras lanzar el programa de instalación nos aparecerá la ventana de bienvenida a la instalación de Lotus Notes, como se puede comprobar en la siguiente imagen, únicamente debemos pinchar sobre *siguiente*.

Figura B.1: Comienzo de instalación de Lotus Notes.

En la siguiente pantalla nos aparecen los términos de Licencia, que tras haber leído la licencia sólo debemos seleccionar sobre *acepto los términos del contrato de licencia*, tal y como aparece reflejado en la siguiente imagen.

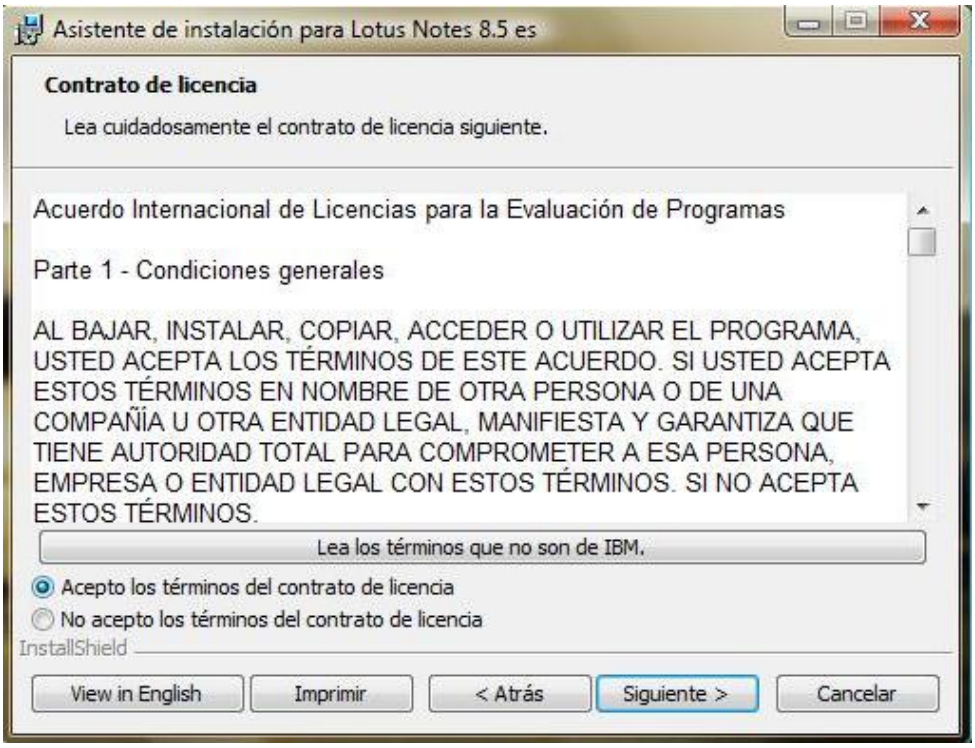

Figura B.2: Contrato de licencia de Lotus Notes.

Tras aceptar los términos de licencia generales, el programa de instalación nos solicitará los datos del cliente que va a instalar la aplicación Lotus Notes, es decir, nos solicita nuestros datos, en nuestro caso los datos son *Nombre de usuario:* David y *Organización:* UC3M, ya que como se trata del proyecto de final de carrera de David Rodríguez Sánchez y que la lectura del mismo se realizará en la Universidad Carlos III de Madrid, hemos creído que eran los mejores datos posibles.

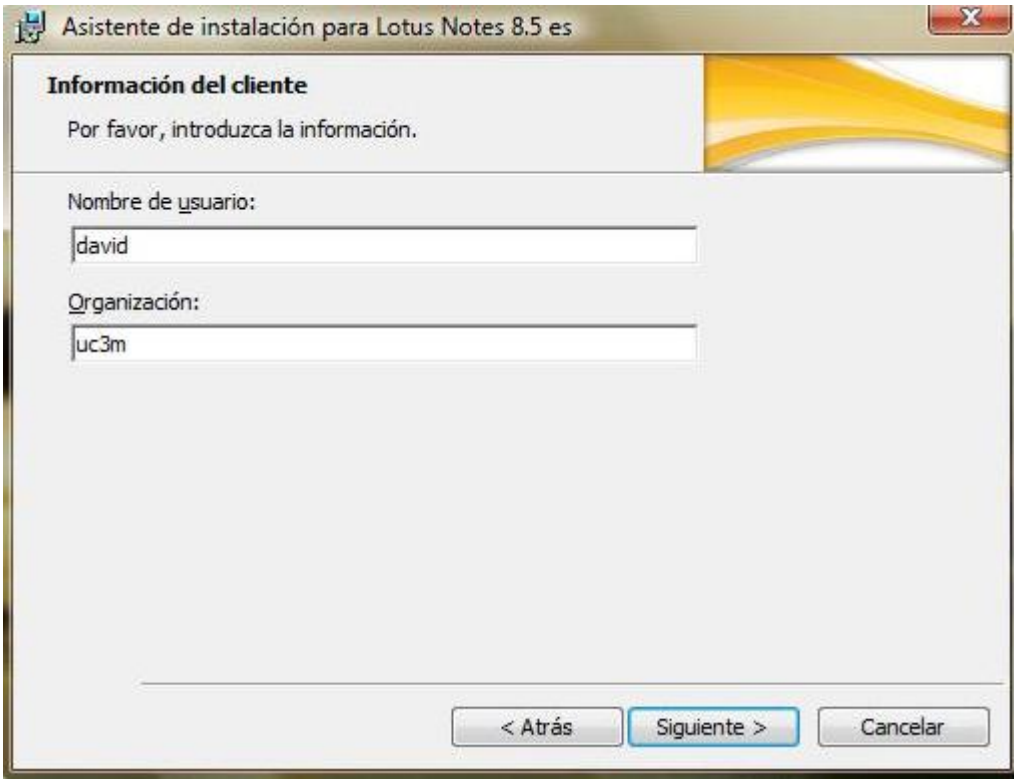

Figura B.3: Datos del cliente.

Seguidamente el programa de instalación de la aplicación Lotus Notes solicita los directorios de programas y de datos en los que se debe instalar la aplicación Lotus Notes, en nuestro caso no hemos modificado los que aparecen por defecto, que como se puede comprobar en la siguiente imagen son

C:\Program Files\IBM\Lotus\Notes y *C:\Program Files\IBM\Lotus\Notes\Data*, respectivamente.

Figura B.4: Directorios de instalación de Lotus Notes.

Tras seleccionar los directorios de instalación deberemos elegir los distintos componentes de la aplicación Lotus Notes que queremos instalar, en la siguiente imagen se pueden observar los diferentes componentes de la aplicación Lotus Notes.

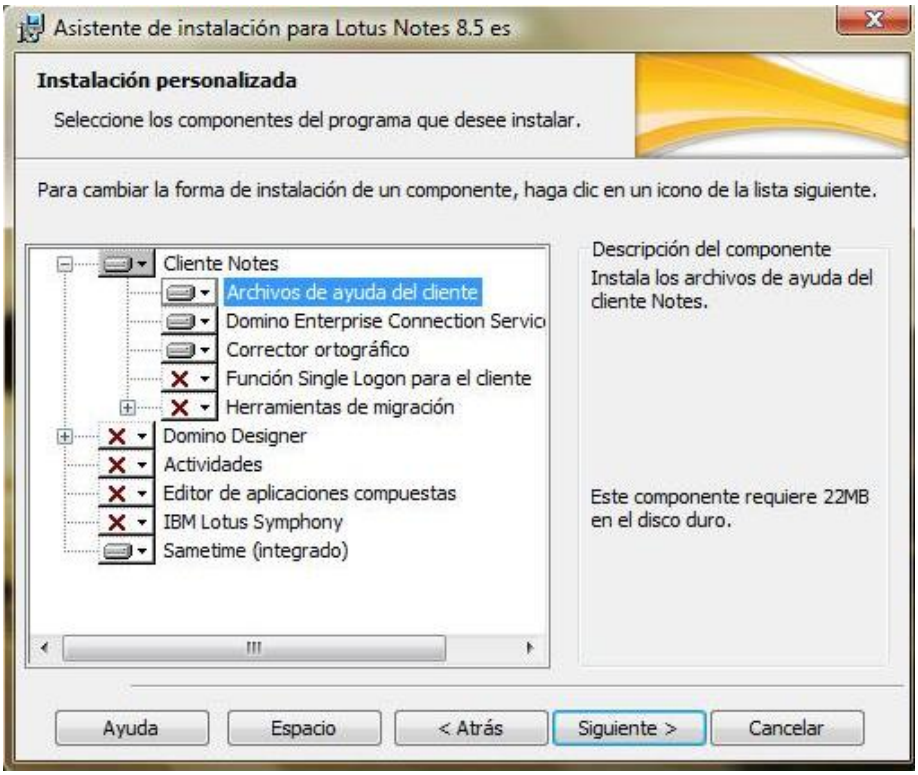

Figura B.5: Componentes de la aplicación Lotus Notes.

El componente *Domino Enterprise Connection Services* instala el soporte para obtener conexión a los servicios de Domino, pero obviamente para tener acceso a los mismos es necesario conectarse a un servidor de Lotus Domino.

El componente *Función Single Logon para el cliente*, como comentamos en el apartado 5 del actual proyecto final de carrera, permite sincronizar la contraseña de Lotus Notes con el inicio de de sesión en Windows.

El componente *Domino Designer* permite diseñar aplicaciones que funcionen bajo la aplicación Lotus Notes, se pueden diseñar aplicaciones muy simples que sean utilizadas únicamente por el usuario que las creó, o aplicaciones más robustas y complejas que puedan ser utilizadas por todos los usuarios de la aplicación Lotus Notes de la organización.

El componente *Actividades*, permite crear tareas compartidas con otros usuarios de la aplicación Lotus Notes y además permite realizar planificaciones

y seguimiento de trabajos por medio de un panel de instrumentos incrustado dentro de la propia aplicación Lotus Notes.

El componente *Editor de aplicaciones compuestas*, permite crear aplicaciones que funcionen sin que la aplicación Lotus Notes se encuentre funcionando, es decir, permite crear aplicaciones que contengan elementos de Lotus Notes, como por ejemplo bases de datos, y que interrelacionen de forma directa con ella desde aplicaciones externa a Lotus Notes.

El componente *IBM Lotus Symphony*, permite crear documentos de texto, hojas de cálculo y presentaciones, además permite visualizar y modificar los documentos creados con Microsoft office.

El componente *Sametime*, permite enviar mensajes instantáneos a otros usuarios de la aplicación Lotus Notes, es un servicio similar al Messenger de Microsoft.

Tras elegir los componentes de la aplicación Lotus Notes que se desean instalar aparecerá la última pantalla del programa de instalación, que se muestra a continuación y en la que podemos seleccionar que la aplicación Lotus Notes sea la aplicación predeterminada para el correo, la agenda y los contactos.

Figura B.6: Finalización de la instalación de Lotus Notes.

Una vez instalada la aplicación Lotus Notes, sólo nos queda configurar el cliente de Lotus Notes para que podamos tener acceso al correo electrónico, a grupos de noticias y a directorios LDAP. En nuestro caso sólo realizaremos la configuración para obtener acceso al correo electrónico, ya que las otras dos opciones no forman parte de la materia del actual proyecto fin de carrera.

Para tener acceso al programa de configuración del cliente Lotus Notes debemos entrar en la aplicación Lotus Notes recién instalada, para ello basta con hacer doble click sobre el icono creado en el escritorio y aparecerá la primera pantalla de la configuración del cliente de Lotus Notes, en esta pantalla únicamente debemos hacer click sobre *siguiente*, tal y como se muestra en la siguiente imagen.

Figura B.7: Configuración del cliente Lotus Notes.

Tras comenzar la configuración del cliente de Lotus Notes, deberemos introducir los datos del usuario que utilizará la aplicación, tal y como se muestra en la siguiente figura, también se debería indicar en esta pantalla el nombre del servidor de Domino que utilizaremos, pero en nuestro caso no disponemos de ninguno.

Figura B.8: Datos del usuario.

En la siguiente pantalla del programa de configuración del cliente de Lotus Notes deberemos seleccionar los servicios que se desean instalar, tal y como se refleja en la siguiente imagen.

Figura B.9.: Servicios que se instalarán.

Como comentamos anteriormente únicamente instalaremos el servicio de correo electrónico, y especificamos el tipo de conexión que utilizaremos.

En la siguiente pantalla del programa de configuración del cliente de Lotus Notes debemos introducir el nombre del servidor de correo electrónico entrante que utilizaremos. En nuestro caso dicho servidor es imap.uc3m.es, que es el servidor corporativo de correo electrónico entrante de la Universidad Carlos III de Madrid al cual tenemos acceso. Como se muestra en la siguiente imagen.

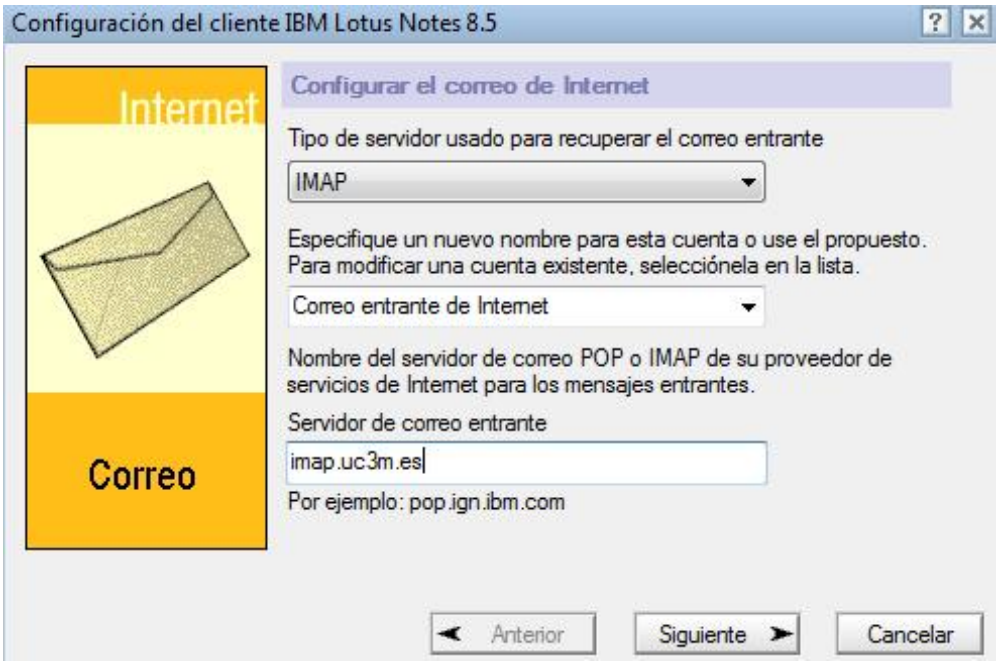

Figura B.10: Configuración del servidor de correo entrante.

En la siguiente pantalla de la configuración del cliente de Lotus Notes debemos introducir los datos de la cuenta de correo y si el acceso a la misma se hará de forma segura a través del protocolo SSL, tal y como se muestra en la siguiente figura.

Figura B.11: Configuración de la cuenta de correo electrónico.

En la siguiente pantalla de configuración del cliente de Lotus Notes debemos introducir los datos del servidor de correo saliente, en nuestro caso será smtp.uc3m.es, que es el servidor corporativo de correo electrónico saliente de la Universidad Carlos III de Madrid, al cual tenemos acceso.

Figura B.12: Configuración del servidor de correo saliente.

En la última pantalla del programa de configuración del cliente de Lotus Notes debemos introducir la dirección completa de correo electrónico y el nombre del dominio de internet al que pertenece dicha cuenta de correo electrónico, tal y como se refleja en la siguiente imagen.

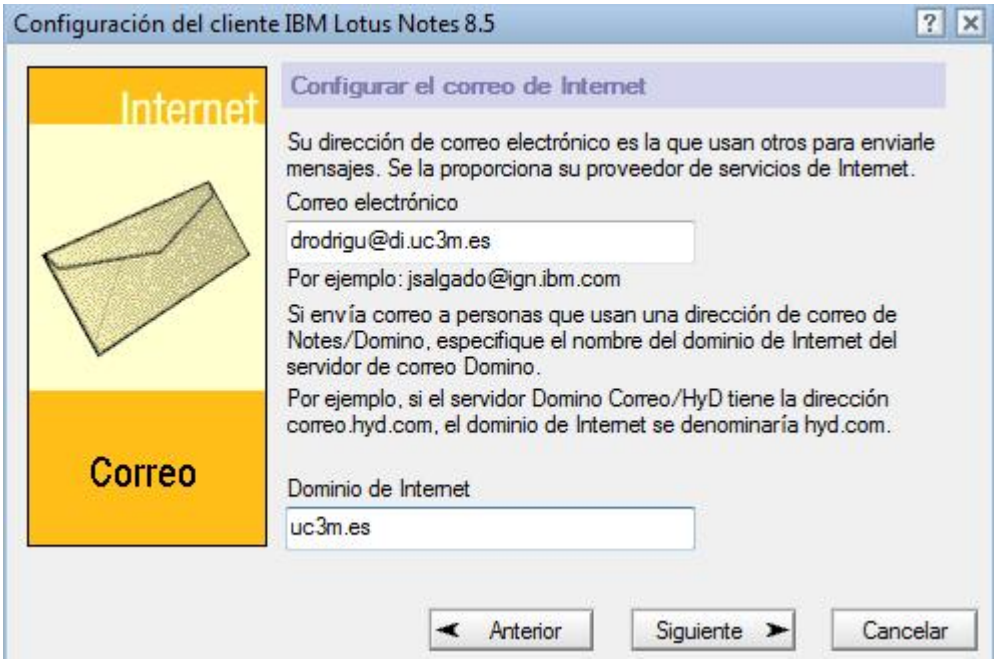

Figura B.13: Datos de la cuenta de correo.

Por fin tenemos instalada y configurada la aplicación Lotus Notes, para poder enviar y recibir correos electrónicos, sólo nos queda entrar en el correo electrónico a través de la aplicación Lotus Notes para comprobar que tenemos acceso a nuestra cuenta de correo y que desde la misma podemos leer nuestros correos electrónicos y enviarlos.

GLOSARIO DE TÉRMINOS.

ADSL o banda ancha:

Es la línea de suscripción digital asimétrica, es decir, es una línea de acceso a internet de forma digital y asimétrica, lo que permite una mayor velocidad de navegación a través de internet.

ARPANET:

Advanced research projects agency network, es la precursora de internet, fue desarrollado por el departamento de defensa de Estados Unidos en el verano de 1.968, y no es más que una gran red de ordenadores conectados a través de la línea telefónica.

ASCII:

American estandar code for information interchange, no es más que un conjunto de caracteres que es utilizado por la mayoría de lenguajes occidentales. Apareció en 1.963, aunque se modificó con posterioridad en 1.967 para incluir algunos caracteres que no fueron incluidos en un primer momento y que si eran utilizados por varios lenguajes.

Backup o copia de seguridad:

Es duplicar la información que se tiene en formato digital a cualquier otro soporte digital para disponer de una copia de la información para su posterior utilización en el caso de que la información original se perdiese o modificase.

Bomba lógica:

Es un tipo de programa malicioso que permanece oculto dentro del código de un programa informático, hasta que se cumple una condición o serie de

condiciones, y a partir de ese momento comienza a ejecutarse de forma automática.

Centro de cálculo o CPD:

Un centro de cálculo o también llamado centro de procesamiento de datos es toda sala habilitada para albergar los recursos necesarios para el procesamiento de información de la organización.

Código de conducta o deontológico:

Es todo conjunto de normas, reglas y valores que engloban cuál debería ser el comportamiento de los profesionales en todo momento.

Computación distribuida:

Son un conjunto de ordenadores interconectados, a través de una red o cualquier otro medio, que funcionan como si se tratase un único ordenador, repartiéndose las diferentes tareas.

Control de acceso biométrico:

Es un tipo de control de acceso que se basa en comprobaciones de las características biológicas, como pueden ser: huellas dactilares, retina,…

Cortafuegos:

Es un programa informático que permite bloquear el acceso de personas no autorizadas, puede ser a nivel de red o del propio sistema operativo.

Dirección IP:

Es un conjunto de números que identifica de forma unívoca un ordenador en internet, y que sirve para que los diferentes ordenadores conectados a internet se puedan comunicar entre sí.

Dominio de internet:

Es el nombre que utilizan los diferentes ordenadores en internet y que está asociado a una o varias direcciones IPs. De esta forma cualquier persona que se quiere conectar a un ordenador a través de internet no tiene que recordar la dirección ip del ordenador, sino que basta con que recuerde el nombre del dominio para conectarse.

EDP Auditors Association:

Es la asociación de auditores de procesamiento de datos electrónicos, que se formó en 1.969 en Los Ángeles (Estados Unidos) y que es uno de los pilares de ISACA.

Encapsulación de datos:

Es toda ocultación de la información en un sistema informático, de forma que sólo se pueda modificar la información en la forma permitida en el sistema informático.

Filtro de correo:

Es una funcionalidad que implementan los gestores de correo, por la cuál es posible discriminar los correos recibidos, en función de alguna característica como el remitente o el asunto, de forma automática.

HTTP:

Hypertext transfer protocol, es el protocolo utilizado en cada transacción web, es decir, define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web.

IBM:

International Bussines Machines, es una empresa multinacional de origen norteamericano dedicada al mundo de la informática

IRPF:

Es el impuesto sobre las personas físicas, que grava la renta obtenida en un año por cada individuo.

ISO:

Es la organización internacional para la estandarización, surgida el 23 de abril de 1.947, y encargada de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación.

LDAP:

Es el protocolo ligero de acceso a directorios, trabaja a nivel de aplicación y permite el acceso a un servicio de directorio ordenado y distribuido para buscar información en una red.

Línea de contención:

Es toda medida cuya finalidad es conseguir una barrera que permita rechazar posibles ataques sobre el sistema.

Lineamiento:

Es toda descripción que aclara el cómo y el qué se debiera hacer para obtener los objetivos establecidos en cualquier política.

Lotus Domino:

Es el nombre que recibe el servidor de la aplicación Lotus Notes.

Messenger:

Es un cliente de mensajería instantánea propiedad de la empresa estadounidense Microsoft.

MIT:

Es el instituto tecnológico de Massachusetts, que es uno de los mayores centros dedicados a la enseñanza y a la investigación dentro de Estados Unidos

Monitorización:

Es el proceso que permite conocer el estado de los sistemas informáticos y del procesamiento de datos realizados por los mismos en todo momento.

Netscape:

Es una empresa estadounidense, cuyo principal mercado es la creación de navegadores web, los más famosos son Netscape y Mozilla-firefox.

NNTP:

Network news transport protocol, es el protocolo encargado de la lectura y publicación de artículos de noticias en internet. Apareció en marzo de 1.986 en la universidad de San Diego (Estados Unidos).

Prestadores de servicios:

Son todas aquellas personas u organizaciones que suministran a un tercero un producto, como pueden ser línea telefónica, corriente eléctrica, gas, agua,..

Puntos de función:

Es una forma de estimar el tamaño definitivo que tendrá un producto software, se basa en el número de iteraciones que tendrá el programa final con los usuarios.

Raíz primitiva:

Sólo los números primos tienen raíces primitivas, y se define como aquel número del conjunto de los números que son menores que el número primo que cumple que al calcular el módulo p de sus potencias sucesivas no se repiten hasta p-1.

RC2:

Es un tipo de algoritmo de cifrado simétrico.

Redundancia del sistema:

Es todo mecanismo que mediante duplicación de componentes permite que el sistema siga funcionando en caso que se produzca un error.

Red Pert:

Es la técnica de revisión y evaluación de programas, que se utiliza para la administración y gestión de proyectos. Fue ideada en 1.958 por la oficina de proyectos especiales de la marina de guerra del departamento de defensa de Estados Unidos.

RFC:

Request for comments, son una serie notas publicadas en internet desde 1.969, en las que se proponen las descripciones de los protocolos utilizados en internet.

Secuestro de sesión:

Es toda interceptación de una comunicación entre varios ordenadores que permite, al interceptor de la comunicación, hacer creer a una de las parte o a varias que el interceptor del la comunicación es uno de los ordenadores que inicialmente formaban parte de la comunicación.

Sistema de alimentación ininterrumpida:

Es un mecanismo que suministra potencia eléctrica, por tiempo limitado, a los sistemas de una organización en caso que por cualquier motivo deje de recibir suministro eléctrico.

Sistema de inteligencia artificial:

Es todo sistema, que debido a su programación especial, puede resolver problemas de forma similar a como los resolvería una persona.

Supercomputadores de tiempo compartido:

Son ordenadores muy potentes que permiten que varios usuarios o procesos tengan acceso simultáneamente a un mismo recurso o información.

Suplantación de identidad:

Es un tipo de ataque sobre los sistemas informáticos que consiste en que una tercera persona, sin autorización para acceder al sistema, trata de acceder al sistema haciendo creer que es un usuario autorizado.

TCP/IP:

Son el protocolo de control de transmisión y de internet respectivamente, se utiliza para interconectar diferentes ordenadores a través de cualquier tipo de red, fueron desarrollados en 1.972.

Telnet:

Telecomunication network, es un protocolo de red que sirve para conectarse a un ordenador a través de una red, para utilizarla de forma remota.

Troyano:

Es un programa malicioso que se ejecuta de forma transparente para el usuario y que permite el acceso remoto al sistema de un tercero no autorizado.

Usuario remoto:

Es un tipo especial de usuario, que no puede acceder de forma local, es decir, para obtener acceso lo hace a través de una red o cualquier otro medio diferente a abrir sesión en el mismo ordenador o terminal.

REFERENCIAS BIBLIOGRÁFICAS.

[1] Auditoría informática de la seguridad física. PFC, S. Lucena. 2.006. 267 p.

[2] Auditoría informática: un enfoque práctico. Ed.: Rama, M. Piattini, E. Peso. 2.001. 660 p.

[3] Auditoría del desarrollo de aplicaciones. PFC. P. Cabañas. 1.994. 139 p.

[4] Ayuda de la aplicación Lotus Notes.

[5] Correo electrónico en internet. Ed.: Paraninfo, J.M. Contreras Alarcón. 1.997. 372 p.

[6] Criptografía digital: fundamentos y aplicaciones. Ed.: Prensas universitarias de Zaragoza, J. Pastor. 2.001. 691 p.

[7] El documento de seguridad. Artículo. E. del Peso. Septiembre 1.999.

[8] Fundamentos de seguridad en redes: aplicaciones y estándares. Ed.: Pearson/Prentice Hall, W. Stallings. 2.004. 418 p

[9] Glosario de términos de las T.I. Ediciones CODA. A. Ribagorda. 1.997. 96 p.

[10] IBM Lotus Notes and Domino 8 Deployment Guide. Noviembre 2.007. 504 p.

[11] Introducción a la criptografía. Ed.: Rama, P. Caballero Gil. 2.002. 133 p.

[12] Introducción a la criptografía: tipos de algoritmos. V. Delgado. 2.006. 46 p.

[13] La auditoría de los datos personales. Artículo. M.A. Ramos. Julio 2.006.

[14] Ley 34/2002 del 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico.

[15] Norma ISO 13335.

[16] Norma ISO 27001.

[17] Norma ISO 27002.

[18] Norma ISO 7498-2.

[19] REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[20] Redes de ordenadores Ed.: Pretice-hall, A. Tanenbauw. 1.991. 759 p.

[21] RFC 733.

[22] RFC 821.

[23] RFC 822.

[24] RFC 1082.

[25] RFC 1176.

[26] RFC 1203.

[27] RFC 1725.

[28] RFC 1730.

[29] RFC 1734.

[30] RFC 1939.

[31] RFC 2045.

[32] RFC 2046.

[33] RFC 2047.

[34] RFC 2060.

[35] RFC 2077.

[36] RFC 2246.

[37] RFC 2821.

[38] RFC 2822.

[39] RFC 4288.

[40] RFC 4289.

[41] Seguridad de la información: redes, informática y sistemas de información. Ed.: Cengage Learning Paraninfo, J. Areitio Bertolín. 2.008. 566 p.

[42] Seguridad y Protección de la información. Ed.: Centro de estudios Ramón Areces, J.L. Morant y A. Ribagorda. 1.994. 388 p.

[43] http://noticias.juridicas.com/

[43] http://es.wikipedia.org

[44] http://www.ibm.es

[45] http://www.iee.es

[46] http://www.isaca.org

[47] http://www.mit.edu