ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Centro de Educación Continua

Diplomado en Auditoría Informática

V PROMOCION

PROYECTO

TEMA:

"Auditoría a la Seguridad de la Información de una Sociedad Financiera"

AUTOR:

Cervantes Bustos Jacinto Geovanny

Año 2011

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACIÓN CONTÍNUA

DIPLOMADO EN AUDITORÍA INFORMÁTICA

V PROMOCIÓN

PROYECTO

TEMA:

"AUDITORÍA A LA SEGURIDAD DE LA INFORMACIÓN DE UNA SOCIEDAD FINANCIERA"

AUTOR

CERVANTES BUSTOS JACINTO GEOVANNY

AÑO

2011

AGRADECIMIENTO

A Dios quien ha sido mi guía y protección en todo lo que he hecho hasta el momento en mi vida. A mis padres por su apoyo incondicional. A la Sociedad Financiera por su apertura y colaboración durante todo este proyecto. A la Mae. Karol Hidalgo por su asesoría durante el desarrollo de este trabajo.

Jacinto Geovanny Cervantes Bustos

DEDICATORIA

A Dios y a mis padres.

Jacinto Geovanny Cervantes Bustos

TRIBUNAL DE GRADUACIÓN

Mae. Jorge Olaya Tapia

Mae. Karol Hidalgo Verdesoto

Mae. Antonio Márquez Bermeo

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Graduación, me corresponde exclusivamente; y el patrimonio intelectual del mismo a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL."

Jacinto Geovanny Cervantes Bustos

RESUMEN

El presente proyecto se ha desarrollado con la finalidad de prever los posibles problemas que se pueden presentar por la ausencia o inadecuada aplicación de controles de seguridad que permitan mantener la información de una institución financiera pequeña a buen recaudo, pues al manejar información monetaria y confidencial, de caer en manos de terceros no autorizados o provocarse la pérdida de la integridad de la misma puede ocasionar un serio impacto e incluso aumentar el riesgo reputacional de la institución, impidiendo cumplir con los objetivos del negocio.

Al ser una institución financiera que depende en gran medida de la tecnología de la información, se incrementan los riesgos que esto conlleva como accesos no autorizados, modificaciones no controladas en los sistemas informáticos, intervención manual inapropiada, pérdida potencial de la información o incapacidad de acceder a la misma.

Por todo esto, la alta gerencia de la sociedad financiera, consciente de la necesidad de evaluar y verificar el cumplimiento de los controles que garanticen que su información se encuentra segura, ha decidido emprender este proyecto para evaluar los controles que permitan garantizar la correcta gestión de la seguridad de la información.

En el presente proyecto se ha realizado el diagnóstico de seguridad de la sociedad financiera, basado en los controles definidos en la norma ISO 27002:2005 a fin de mejorar sus procesos y garantizar la integridad, confidencialidad y disponibilidad de la información sensible que maneja.

ÍNDICE GENERAL

CAPÍTULO **Pág.**

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

Pág.

Capítulo 1
Introducción

1. INTRODUCCIÓN

1.1. ANTECEDENTES

El presente proyecto de graduación es una "Auditoría a la Seguridad de la Información de una Sociedad Financiera", la cual va a permitir realizar un diagnóstico a la seguridad de la información basado en la norma ISO 27002:2005.

Al ser una institución financiera que depende en gran medida de la tecnología de la información, si ésta tecnología no se somete a los controles adecuados, puede ocasionar que los riesgos derivados de errores de procesamiento manual se materialicen en fallos en el sistema.

1.2. JUSTIFICACIÓN

La justificación del desarrollo de este proyecto se da por la existencia de riesgos que pueden afectar a la información con las consecuencias negativas que esto conlleva; entre los riesgos más comunes están los hackers, virus, fraudes internos, fraudes externos, catástrofes o emergencias.

Cabe mencionar:

- Que cada año las organizaciones pierden alrededor del 5% de sus ingresos a causa de fraudes.
- El promedio de las pérdidas causadas por fraudes de empleados es de $160,000, pero un cuarto del total llega al millón de dólares.

- El fraude típico tarda en descubrirse 18 meses.
- Mientras controles más inteligentes implementan las empresas, menos fraudes experimentan.

Prácticamente las instituciones financieras coinciden en que, dentro de los llamados ilícitos patrimoniales más frecuentes en su contra, resalta el fraude en sus diversas modalidades.

Esto acaba con la confianza de los clientes, lo que conlleva a que muchos bancos cierren sus puertas definitivamente y que otros se fusionen para continuar ofreciendo sus servicios al público.

Entre los más importantes están: el fraude genérico, el específico y el informático; el fraude con el uso de tarjetas de débito o de crédito falsas; el uso de cheques falsos, de cheques originales obtenidos de forma ilícita; el desvío de fondos destinados al pago de impuestos y los accesos indebidos a los sistemas informáticos de las Instituciones financieras con la finalidad de realizar transferencias ilegales de recursos a través de Fraudes Internos y en algunos casos Fraudes Externos.

Desde el año 2010 en el Ecuador se han reportado una serie de fraudes electrónicos que se han materializado a través de los portales web transaccionales de las

instituciones financieras, de allí la importancia de poner mayor interés en estos temas de seguridad e incluso de capacitación tanto del cliente interno como externo.

Actualmente tanto el control interno como la Auditoría son totalmente necesarios y, si estos son aplicados correctamente ayudan en forma oportuna a la organización para no ser el blanco de ilícitos o de pérdidas importantes de información a fin de detectar las oportunidades de mejora necesarias para fortalecer la seguridad de la información.

Capítulo 2

Marco Teórico y Conceptual

2. MARCO TEÓRICO Y CONCEPTUAL

2.1. METODOLOGÍAS USADAS

Diagnóstico de seguridad basado en la norma ISO 27002:2005; cumpliendo con las siguientes fases:

1. Definir el alcance de la Auditoría: Análisis Inicial y Programa de Auditoría
2. Recopilación de información, identificación y realización de pruebas de auditoría, incluyendo, si se acuerda, análisis de vulnerabilidad de aplicaciones.
3. Análisis de las evidencias, documentación de los resultados obtenidos y conclusiones.
4. Informe de Auditoría en el que se recogen las acciones realizadas a lo largo de la auditoría y las oportunidades de mejora detectadas en materia de seguridad de la información.
5. Plan de Mejora con el análisis y las recomendaciones propuestas para subsanar las incidencias de seguridad encontradas y mantener en el futuro una situación estable y segura de los sistemas de información.

2.2. TÉRMINOS Y DEFINICIONES

2.2.1. ISO 27001

ISO/IEC 27001 es una norma desarrollada por ISO (Internacional Organization for Standardization) e IEC (International Electrotechnical Commission), que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Está orientada a aspectos netamente organizativos, por ello propone toda una secuencia de acciones tendientes al establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS (Information Security Management System).

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:

- ✓ ISMS
- ✓ Valoración de riegos (Risk Assesment)
- ✓ Controles

2.2.2. FAMILIA DE LAS ISO 27000

ISO 27001

Es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de

Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA (Plan, Do, Check, Act) al igual que otras normas de sistemas de gestión. Es un estándar certificable, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

ISO 27002

Su origen está en la norma de BSI (British Standards Institution) BS7799 Parte 2, norma que fue publicada por primera vez en 1998 y ya era un estándar certificable desde entonces. No es certificable.

ISO 27003

Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004

Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan

fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

ISO 27005

Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la seguridad de la información.

ISO 27006

Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

ISO 27007

Consiste en una guía de auditoría de un SGSI.

ISO 27011

Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031

Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032

Consiste en una guía relativa a la cyberseguridad.

ISO 27033

En fase de desarrollo; su fecha prevista de publicación es este año 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de

comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y renumeración de ISO 18028.

ISO 27034

Consiste en una guía de seguridad en aplicaciones.

ISO 27799

Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799. Esta norma la desarrolla el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. Especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. Se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas.

2.2.3. ADAPTACIÓN A LA NORMA

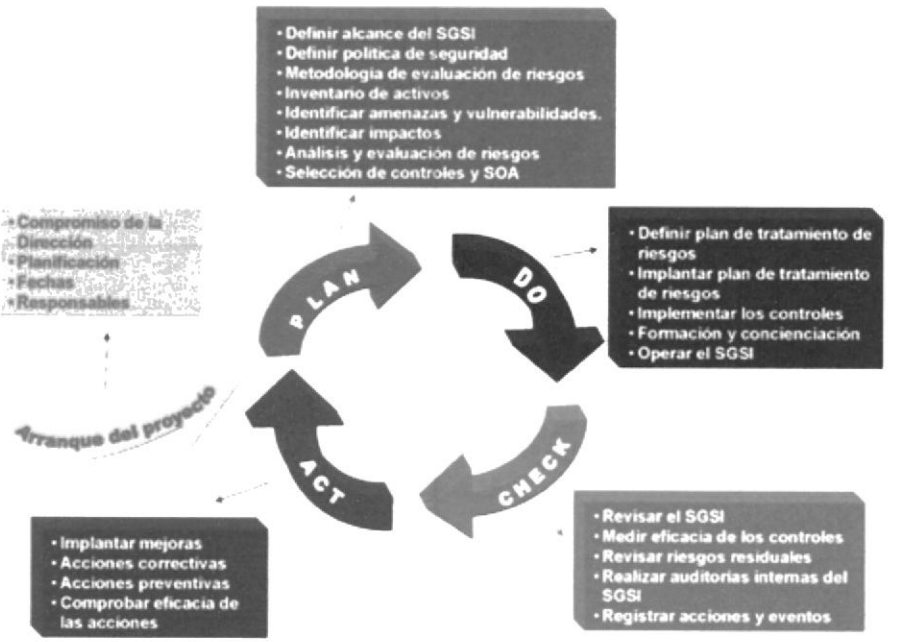

Figura 2.1. Cómo adaptarse a la Norma ISO 27001

Compromiso de la Dirección: una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado en la norma sino porque el cambio de cultura y concienciación hacen necesario el impulso constante de la Dirección.

2.2.4. MOTIVO PARA IMPLEMENTAR LA NORMA

Porque para una adecuada gestión de la seguridad de la información, es necesario implantar un sistema que permita el aseguramiento de la información y de los sistemas que la procesan, de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

2.2.5. BENEFICIOS DE IMPLEMENTAR LA NORMA

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas (ISO 9001, ISO 14001, OHSAS 18001L).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.

- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

2.2.6. TIPOS DE EMPRESAS QUE SE ESTÁN CERTIFICANDO

El estándar se puede adoptar por la mayoría de los sectores comerciales, industriales y de servicios de pequeñas, medianas o grandes entidades y organizaciones: finanzas, aseguradoras, telecomunicaciones, servicios públicos, minoristas, sectores de manufactura, industrias de servicios diversos, sector del transporte y gobiernos entre otros.

En la actualidad destaca su presencia en 46 empresas sudamericanas dedicadas principalmente a servicios y consultorías de tecnologías de la información, telecomunicaciones e instituciones financieras como prueba del compromiso con la seguridad de los datos de sus clientes.

2.2.7. EMPRESAS CERTIFICADAS EN EL MUNDO

A nivel mundial a Junio del 2011, existen 7289 instituciones certificadas en la norma ISO 27001, cabe resaltar que en el Ecuador existe 1 institución certificada en la norma (Telconet S.A.). En el siguiente gráfico se muestran los países con mayor cantidad de empresas certificadas:

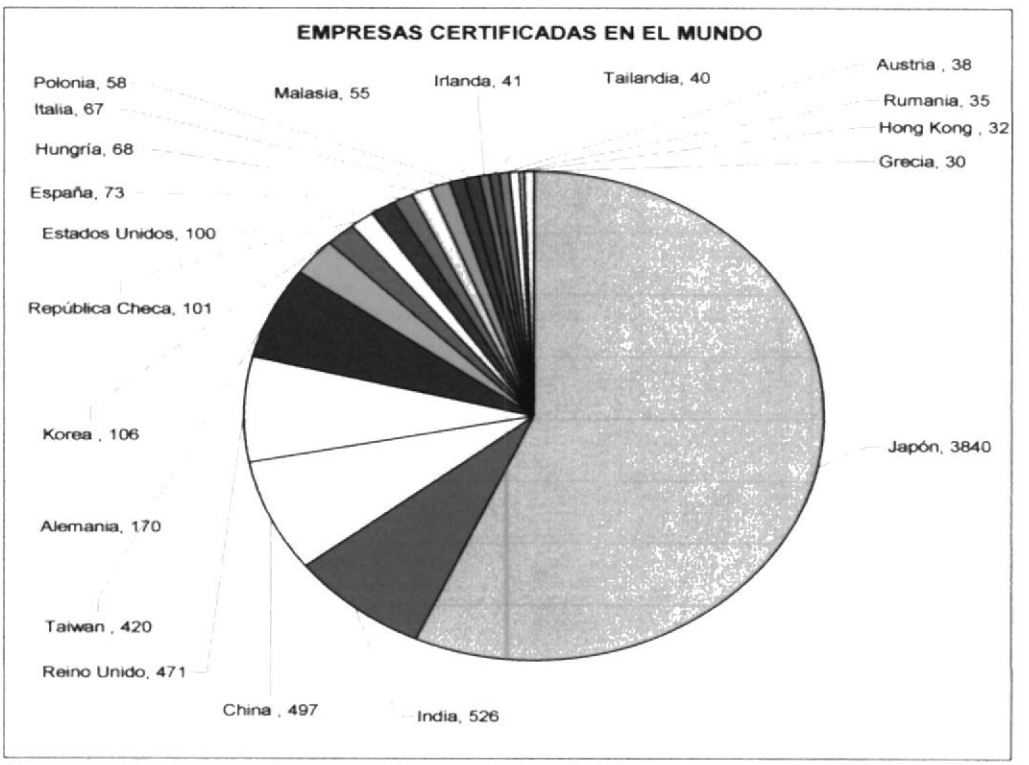

Figura 2.2. Empresas certificadas en el mundo

2.2.8. EMPRESAS CERTIFICADORAS A NIVEL MUNDIAL

Entre las principales empresas certificadoras están:

Figura 2.3. Empresas certificadoras a nivel mundial

2.2.9. DOMINIOS DE ISO 27002:2005

A continuación se presenta un breve resumen en base a los 11 dominios, 39 objetivos de control y 133 controles que se manejan en ISO 27002:2005 y en los cuáles se va a basar la auditoría que se va a realizar en la institución.

Política de Seguridad

Objetivo	Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.
Principios	La Dirección debe establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.

Métrica	Cobertura de la política (es decir, porcentaje de secciones de ISO/IEC 27001/2 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoría, gerencia o auto-evaluación).

Tabla 2.1.: Política de Seguridad

Aspectos Organizativos

Objetivo	Gestionar la seguridad de la información dentro de la Organización tanto interna como externa.
Principios	Establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización. El órgano de dirección debe aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implantación de la seguridad en toda la Organización. Si fuera necesario, en la Organización se debería establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad. Control de acceso de terceros a los dispositivos de tratamiento de información de la organización. Cuando el negocio requiera dicho acceso de terceros, se debe realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deberían definirse y aceptarse en un contrato con la tercera parte.
Métrica	Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado

	formalmente, roles y responsabilidades de seguridad de la información. Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.

Tabla 2.2.: Aspectos Organizativos

Gestión de Activos

Objetivo	Alcanzar y mantener una protección adecuada de los activos de la Organización y asegurar que se aplica un nivel de protección adecuado a la información (clasificación).
Principios	Todos los activos deben ser justificados y tener asignado un propietario. Identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados. La implantación de controles específicos podría ser delegada por el propietario convenientemente. Se debe clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento. Debe utilizarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.
Métrica	Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado). Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y para mantener dichos riesgos en niveles aceptables. Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar").

Tabla 2.3.: Gestión de Activos

Recursos Humanos

Objetivo	Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan: ✓ Sus responsabilidades y sean aptos para las funciones que desarrollen. ✓ Se encuentren equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos. ✓ Entiendan la política para el abandono de la organización o cambio de empleo en forma organizada. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.
Principios	Definir responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización. Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo. Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes deben ser seleccionados adecuadamente, especialmente para los trabajos sensibles. Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deben firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad. A todos los usuarios empleados, contratistas y terceras personas se les debería proporcionar un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad. Se deberían establecer las responsabilidades para asegurar que el abandono de la organización por parte de los empleados, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso.

Métrica	Porcentaje de nuevos empleados o pseudo-empleados (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar. Respuesta a las actividades de concienciación en seguridad. Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).

Tabla 2.4.: Recursos Humanos

Física y Ambiental

Objetivo	Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización (áreas seguras). Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización (seguridad de equipos).
Principios	Los servicios de procesamiento de información sensible deben ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias. La protección suministrada debe estar acorde con los riesgos identificados. Protección de los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo. Así mismo, se debe considerar la ubicación y eliminación de los equipos. Se pueden requerir controles especiales para la protección contra amenazas físicas y para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.
Métrica	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún

	estén pendientes. Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.

Tabla 2.5.: Física y Ambiental

Comunicaciones y Operaciones

Objetivo	Procedimientos y responsabilidades de: operación, gestión de servicios de terceras partes, planificación y aceptación del sistema, protección contra software malicioso, backup, gestión de seguridad de redes, utilización de soportes de información, intercambio de información y software, servicios de comercio electrónico y monitorización.
Principios	Se deben establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información. Segregación de tareas cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia. La organización debe verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros. Se requiere una planificación y preparación avanzadas para garantizar la adecuada capacidad y recursos con objeto de mantener la disponibilidad de los sistemas requerida. Realizar proyecciones de los requisitos de capacidad en el futuro para reducir el riesgo de sobrecarga de los sistemas. Se deben establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los nuevos sistemas. Se requiere de ciertas precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados. Los usuarios deben conocer los peligros que puede ocasionar el software malicioso o no autorizado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción.

	Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización. Decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes. Encriptar copias de seguridad y archivos que contengan datos sensibles o valiosos.
Métrica	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo que ha llevado parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchar por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón). Costo del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, costo, etc. Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos. Porcentaje de sistemas (a) Que deberían cumplir con estándares de seguridad básica o similar y (b) Cuya conformidad con dichos estándares ha sido comprobada mediante benchmarking o pruebas. Tendencia en el número de virus, gusanos, troyanos o spam detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso. Porcentaje de operaciones de backup exitosas. Porcentaje de recuperaciones de prueba exitosas. Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales. Porcentaje de backups y archivos con datos sensibles o valiosos que están encriptados.

Tabla 2.6.: Comunicaciones y Operaciones

Control de Accesos

Objetivo	Requisitos de negocio para el control de accesos, gestión de acceso de usuario, responsabilidades del usuario, control de acceso en red, control de acceso al sistema operativo, control de acceso a las aplicaciones e informaciones, informática y conexión móvil.
Principios	Control de los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización. Para las regulaciones para el control de los accesos se deben considerar las políticas de distribución de la información y de autorizaciones. Establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Los procedimientos deben cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información. Se debe prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema. Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición. Implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información. Control de los accesos a servicios internos y externos conectados en red. El acceso de los usuarios a redes y servicios en red no debe comprometer la seguridad de los servicios en red si se garantizan: a) Que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras

	organizaciones; b) Que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos; c) El cumplimiento del control de los accesos de los usuarios a los servicios de información. Utilizar las prestaciones de seguridad del sistema operativo para permitir el acceso exclusivo a los usuarios autorizados. Las prestaciones deberían ser capaces de: a) La autenticación de los usuarios autorizados, de acuerdo a la política de control de accesos definida; b) Registrar los intentos de autenticación correctos y fallidos del sistema; c) Registrar el uso de privilegios especiales del sistema; d) Emitir señales de alarma cuando se violan las políticas de seguridad del sistema; e) Disponer los recursos adecuados para la autenticación; f) Restringir los horarios de conexión de los usuarios cuando sea necesario. Utilizar dispositivos de seguridad con objeto de restringir el acceso a las aplicaciones y sus contenidos. Restringir el acceso lógico a las aplicaciones software y su información únicamente a usuarios autorizados. Los sistemas de aplicación deben: a) Controlar el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida; b) Proporcionar protección contra accesos no autorizados derivados del uso de cualquier utilidad, software del sistema operativo y software malicioso que puedan traspasar o eludir los controles del sistema o de las aplicaciones; c) No comprometer otros sistemas con los que se compartan recursos de información. Tener políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles (es decir, laptops, PDAs, etc.), sino, en mayor medida, de la información

	almacenada en ellos. Por lo general, el valor de la información supera con mucho el del hardware. Asegurar que el nivel de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como antivirus, parches, actualizaciones, software cortafuegos, etc.
Métrica	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) Sido identificados, (b) Aceptado formalmente sus responsabilidades, (c) Llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) Definido las reglas de control de acceso basadas en roles. Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior. Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información: (a) Totalmente documentadas y (b) Formalmente aceptadas. Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos). Estadísticas de vulnerabilidad de sistemas y redes, como número de vulnerabilidades conocidas cerradas, abiertas y nuevas; velocidad media de parcheo de vulnerabilidades (analizadas por prioridades/categorías del fabricante o propias). Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes. Un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (laptops, PDAs, teléfonos móviles, etc.), y de teletrabajo (en casa de los empleados, fuerza de trabajo móvil), con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos

	sobre cualquier riesgo creciente, despliegue de configuraciones seguras, antivirus, firewalls personales, etc.

Tabla 2.7.: Control de Accesos

Adquisición, desarrollo y mantenimiento de sistemas

Objetivo	Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas. (Garantizar la seguridad integral de los sistemas)
Principios	El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información. Todos los requisitos de seguridad deben identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información. Diseñar controles apropiados en las propias aplicaciones, incluidas las desarrolladas por los propios usuarios, para asegurar el procesamiento correcto de la información. Estos controles deben incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida. Pueden ser requeridos controles adicionales para los sistemas que procesan o tienen algún efecto en activos de información de carácter sensible, valioso o crítico. Dichos controles deben ser determinados en función de los requisitos de seguridad y la estimación del riesgo. Desarrollar una política de uso de controles criptográficos. Establecer una gestión de claves que de soporte al uso de de técnicas criptográficas. Controlar el acceso a los sistemas de ficheros y código fuente de los programas. Los proyectos TI y las actividades de soporte deben ser dirigidos de un modo seguro. Evitar la exposición de datos sensibles en entornos de prueba.

	Controlar estrictamente los entornos de desarrollo de proyectos y de soporte. Los directivos responsables de los sistemas de aplicaciones deben ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deben garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo.
Métrica	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) Definido y (b) Implementado y demostrado eficacia mediante pruebas. Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados (periodo de reporte de 3 a 12 meses). Porcentaje de sistemas evaluados de forma independiente como totalmente conformes con los estándares de seguridad básica aprobados, respecto a aquellos que no han sido evaluados, no son conformes o para los que no se han aprobado dichos estándares. Estado de la seguridad en sistemas en desarrollo, es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.

Tabla 2.8.: Adquisición, desarrollo y mantenimiento de Sistemas

Gestión de incidentes

Objetivo	Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.
Principios	Establecerse el informe formal de los eventos y de los procedimientos de escalada. Todos los empleados, contratistas y terceros deben estar al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales. Se debe exigir que informen de cualquier evento o debilidad en la seguridad de información lo más rápido posible y al punto de contacto designado. Establecer responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados. Aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información. Cuando se requieran evidencias, éstas deben ser recogidas para asegurar el cumplimiento de los requisitos legales.
Métrica	Estadísticas del helpdesk de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, crear y publicar una tabla de clasificación por departamento, mostrando aquellos que están claramente concienciados con la seguridad frente a los que no lo están. Número y gravedad de incidentes; evaluaciones de los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida. Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección.

Tabla 2.9.: Gestión de Incidentes

Gestión de Continuidad del negocio

Objetivo	Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.
Principios	Implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación. Identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones. Analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales. La seguridad de información debe ser una parte integral del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la organización. La gestión de la continuidad del negocio debe incluir adicionalmente al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación a tiempo de las operaciones esenciales.
Métrica	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado). Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) Documentados y (b) Probados mediante tests apropiados en los últimos 12 meses.

Tabla 2.10.: Gestión de Continuidad del negocio

Cumplimiento legal

Objetivo	Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.
Principios	Los requisitos legales específicos deben ser advertidos por los asesores legales de la organización o por profesionales adecuadamente calificados. Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras). Realizar revisiones regulares de la seguridad de los sistemas de información. Las revisiones se deben realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados. Deben existir controles para proteger los sistemas en activo y las herramientas de auditoría durante el desarrollo de las auditorías de los sistemas de información. También se requiere la protección para salvaguardar la integridad y prevenir el mal uso de las herramientas de auditoría.
Métrica	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes. Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales. Número de cuestiones o recomendaciones de auditoría, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).

	Porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo. Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorías.

Tabla 2.11.: Cumplimiento Legal

Capítulo 3

Desarrollo del Programa de Auditoría

3. DESARROLLO DEL PROGRAMA DE AUDITORÍA

3.1. INVESTIGACIÓN PRELIMINAR

3.1.1. RESEÑA HISTÓRICA

La Sociedad Financiera fue constituida en Ecuador en julio 22 de 1988. Es una institución financiera regulada por la Superintendencia de Bancos y Seguros, con más de 20 años de experiencia en el mercado, satisfaciendo las necesidades de crédito e inversiones.

En el año 1995 define el nuevo modelo y estrategia de negocios, especializándose en el Crédito Vehicular e Inversiones en Depósitos a Plazo.

A Abril del 2011 posee la calificación "A+" otorgada por Humphreys S.A.

Cuenta con una oficina en Guayaquil ubicada en el Centro Comercial Aventura Plaza Local 10.

3.1.2. MISIÓN

Proporcionar productos y servicios financieros de calidad, con un equipo profesional, capacitado, ético y eficiente, que satisfaga las necesidades bancarias de los clientes.

Comprometida con garantizar rentabilidad, seguridad y solvencia a quienes se relacionen financieramente con la empresa.

3.1.3. VISIÓN

Ser líderes en la concesión de créditos personales, en la región Costa del País, aplicando el asesoramiento profesional personalizado para obtener la satisfacción, confianza y lealtad de nuestros clientes.

3.1.4. SERVICIOS CLAVES

- Créditos Comerciales
- Créditos de Consumos (Vehiculares)
- Microcréditos
- Inversiones (Depósitos a Plazo Fijo)

3.1.5. ORGANIGRAMA DE LA EMPRESA

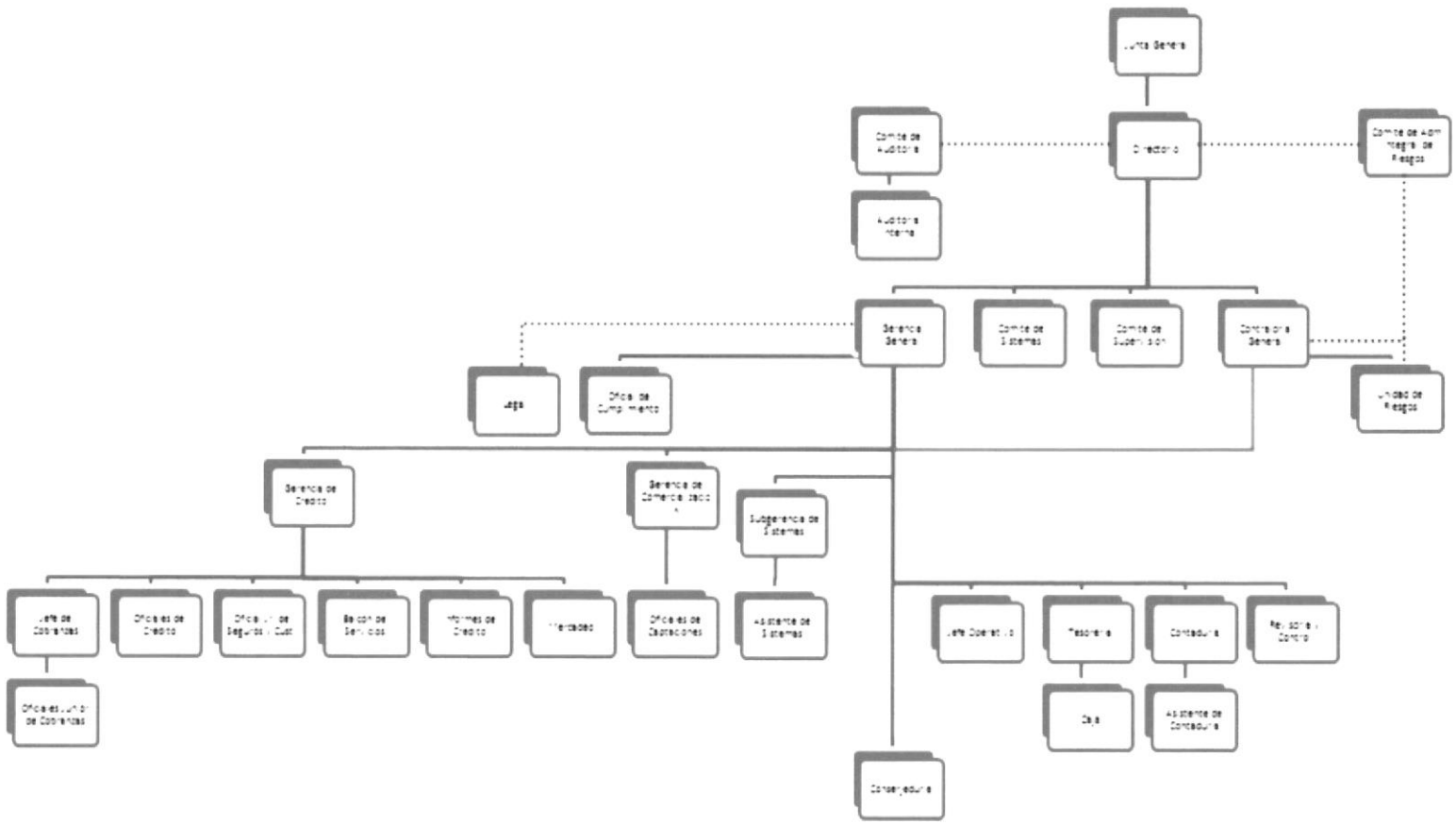

Figura 3.1. Organigrama de la empresa

3.1.6. AMBIENTE DE SISTEMAS

La empresa posee un Departamento de Sistemas el cual está integrado por 2 personas: el Subgerente de Sistemas y un Analista-Programador de Sistemas. La subgerencia de Sistemas reporta directamente a Contraloría.

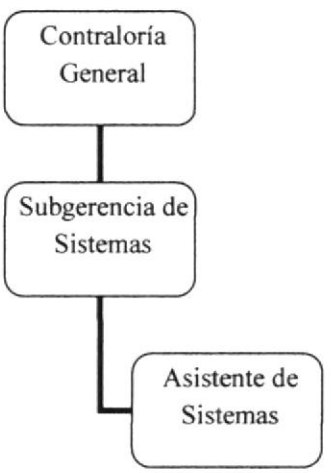

Figura 3.2. Organigrama del Área de Sistemas

3.1.7. TECNOLOGÍA DE LA INFORMACIÓN

Entre los servicios tecnológicos que brinda están:

- Administración y soporte especializado de la red corporativa y base de datos.

  Este servicio se refiere al monitoreo del rendimiento y correcto funcionamiento de la red y de la base de datos.

- Desarrollo de aplicaciones

  Este servicio contempla todo el proceso de desarrollo o mantenimiento de aplicaciones comenzando por el análisis y concluyendo con las pruebas y puesta en producción de las aplicaciones.

- Soporte a Usuarios

  Se refiere al soporte al cliente interno o helpdesk que brinda el Departamento de Sistemas.

- Correo electrónico

  Este servicio contempla la administración de las cuentas de correo y la administración del espacio ocupado en disco por cada usuario en el servidor de correos.

- Acceso a Internet

  Este servicio se refiere a la administración del acceso a internet: permisos, bloqueos a páginas web, etc.

3.1.8. PLATAFORMA IT

Para cumplir con los objetivos del negocio el departamento de sistemas tiene implementado 4 servidores detallados a continuación:

Servidor	Sist. Operativo	Ubicación	Información
Producción	Linux	Gabinete de Servidores	Base de Datos principal y sistema de Contabilidad y Cartera.
Dominio	Windows Server 2003	Gabinete de Servidores	Bases de Datos de aplicaciones satélites, respaldos de usuarios y carpetas compartidas por departamento con sus respectivos permisos de usuario.
Internet	Linux	Gabinete de Servidores	Configuraciones y reglas de acceso a internet (por IP y por páginas).
Desarrollo	Linux	Gabinete de Servidores	Base de Datos de Desarrollo
Contingencias	Linux	Instalaciones de Sistecom (El Oro y la Ría)	Base de Datos principal y sistema de Contabilidad y Cartera

Tabla 3.1.: Plataforma IT

3.1.9. APLICACIONES

La institución posee un sistema principal (adquirido) y varias aplicaciones "satélites". El sistema principal es el Sistema de Cartera y Contabilidad pues toda la información de las aplicaciones "satélites" se integra y consolida en la base de datos de este sistema manteniendo la información actualizada y centralizada en esta base

de datos y es desde aquí donde se generan la mayor parte de las estructuras de datos que se envían a los entes de control. El sistema de Cartera y Contabilidad se encuentra desarrollado en Acu-Cobol y como base de datos Oracle y fue desarrollado por la empresa Sistecom S.A. sin embargo, el mantenimiento de este sistema se lo realiza internamente.

Los sistemas "satélites" son los siguientes:

Sistema	Lenguaje	Base de Datos	Desarrollo
Depósitos a Plazo	Visual Basic 6.0	Access	Interno
Inversiones	Visual Basic 6.0	Access	Interno
Riesgos de Mercado y Liquidez	Power Builder	Mysql	Scalar Consulting
Riesgo Operativo	Power Builder	Oracle	Scalar Consulting
Riesgo de Crédito	Power Builder	Oracle	Scalar Consulting
Activos Fijos	Visual Basic 6.0	Access	Interno
Proveeduría	Visual Basic 6.0	Access	Interno
Nómina	Visual Basic 6.0	Access	Interno
RRHH	Visual Basic 6.0	Access	Interno
Informes	Visual Basic 6.0	Access	Interno
Clientes y Liquidaciones de Crédito	Visual Basic 6.0	Oracle	Interno

Tabla 3.2.: Sistemas "satélites"

3.1.10. VOLUMEN DE TRANSACCIONES

El volumen mensual promedio de transacciones en el sistema de Cartera y Contabilidad, de acuerdo a lo indicado por el Subgerente de Sistemas en reunión inicial mantenida, es aproximadamente:

Sistema	# de transacciones Aproximado
Cartera	200
Contabilidad	300
Total	**500**

Tabla 3.3.: Volumen de transacciones mensual

3.2. EVALUACIÓN DE RIESGOS

A continuación se presenta la evaluación de riesgos realizada de acuerdo a los dominios que se van a evaluar.

Dominio	Vulnerabilidad	Riesgo
Política de Seguridad	Que falte compromiso por parte de la Alta Gerencia en apoyar al mantenimiento y cumplimiento de la política de Seguridad.	Que la aplicación de la política no sea adecuada, lo cual puede comprometer la integridad, confidencialidad y disponibilidad de la información.
	Que no esté definido un proceso disciplinario (sanciones) por violaciones a las políticas de seguridad.	Que se violen las políticas de Seguridad al saber que no existe formalmente una sanción.

Dominio	Vulnerabilidad	Riesgo
Organización de la Seguridad de la información	Que los temas de seguridad sean de responsabilidad exclusiva del Área de Sistemas.	Que la aplicación de las políticas de seguridad no sean efectivas.
	Que no estén definidas las responsabilidades del Oficial de Seguridad.	Que no exista responsabilidad en los Controles de Seguridad de la información. Que no se cumplan las políticas de seguridad poniendo en riesgo los criterios de información de disponibilidad, integridad y confidencialidad.
	Que no existan procedimientos para cambio de equipos.	Pérdida de la confidencialidad de la información.
Gestión de Activos	Que no se cuente con un inventario de activos que permita identificar sus características y responsables de los mismos.	Pérdida de equipos y de la información contenida en los mismos, poniendo en riesgo la confidencialidad de la información.
	Que la información no se encuentre correctamente etiquetada e identificada.	Pérdida de la confidencialidad de la información.
Seguridad de los recursos humanos	Que las funciones y responsabilidades del personal no se encuentren definidas (roles y perfiles de usuario).	Accesos no autorizados. Robo, fraude o mal uso de la información a su cargo. Pérdida de la confidencialidad e integridad de la información. Imposibilidad de detectar oportunamente posibles violaciones de seguridad.
	Falta de capacitación en temas de Seguridad de la Información.	Error humano por falta de conocimiento que puede afectar a la integridad o confidencialidad de la información.
Seguridad física	Inexistencia de controles de entrada físicos al Centro de Cómputo.	Accesos no autorizados que puedan ocasionar de forma intencionada o no,

Dominio	Vulnerabilidad	Riesgo
		alteraciones en las actividades normales de procesamiento o extracción de información sensitiva para la institución.
	Falta de protección física contra daños ambientales o creados por el hombre.	Pérdidas o daños irreparables en los recursos de información al presentarse desastres y no estar preparados, con lo cual se puede poner en riesgo la disponibilidad de la información.
	Falta de procedimientos para manejo de equipos fuera de la institución.	Accesos no autorizados.
	Falta de procedimientos para la eliminación segura de equipos.	Pérdida de la confidencialidad de la información.
	Que no existan autorizaciones para trasladar equipos.	Accesos no autorizados y pérdida de la confidencialidad de la información.
Gestión de las comunicaciones y operaciones	Que no se cuente con la suficiente de documentación relativa a los procedimientos de operación.	No ejecución de procesos claves que afecten a la integridad y disponibilidad de la información.
	Que no exista un procedimiento formal de control de cambios en los sistemas informáticos.	Ejecución de programas sin autorización que afecten a la integridad y disponibilidad de la información.
	Inadecuada segregación de funciones.	Robo, fraude o mal uso de la información a su cargo. Imposibilidad de detectar oportunamente posibles violaciones de seguridad.
	Que no se encuentren separados los ambientes de desarrollo y producción.	Accesos y ejecución de programas no autorizados.
	Que no existan controles de seguridad, definiciones de servicio y niveles de	Que no se cuente con los equipos o servicios necesarios para el

Dominio	Vulnerabilidad	Riesgo
	entrega incluidos en contratos de terceros.	desarrollo normal de las operaciones lo que puede afectar a la integridad y disponibilidad de la información.
	Que no se realicen monitoreos a la capacidad de los recursos.	Fallas en los sistemas o equipos que afectan a la disponibilidad e integridad de la información.
	Que no existan controles contra software malicioso (Virus)	Pérdida de la integridad y disponibilidad en los sistemas y en la información.
	Que no se realicen respaldos de la información y software esencial.	Pérdida de la integridad y disponibilidad en los sistemas y en la información, pudiendo poner en riesgo la continuidad del negocio.
	Que no existan procedimientos para la gestión de medios removibles.	Pérdida de la confidencialidad de la información almacenada en medios removibles.
	Que no existan procedimientos para la eliminación de medios removibles.	Pérdida de la confidencialidad de la información almacenada en medios removibles.
	Que no existan controles para proteger la documentación del sistema.	Divulgación no autorizada que afecta a la confidencialidad de la información.
	Ausencia de logs de auditoría.	Imposibilidad de detectar oportunamente posibles violaciones de seguridad.
	Ausencia de bitácoras de operaciones	Imposibilidad detectar oportunamente posibles actividades de procesamiento de información no autorizadas.
Control de acceso	Ausencia de un procedimiento para el registro de nuevos usuarios y asignación de privilegios.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.
	Que no exista un	Accesos no autorizados

Dominio	Vulnerabilidad	Riesgo
	procedimiento formal para la asignación de claves.	que pueden afectar a la confidencialidad e integridad de la información.
	Que no se revisen los derechos de acceso de los usuarios utilizando un proceso formal.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.
	Que no existan buenas prácticas en el uso de claves.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.
	Que no exista protección al equipo desatendido.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.
	Que no se cuente con una política de pantalla y escritorio limpios.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.
	Que no exista autenticación de usuario en el terminal.	Accesos no autorizados al Sistema Operativo del terminal.
	Que las sesiones de usuario queden activan luego de un largo periodo de inactividad.	Accesos no autorizados al Sistema Operativo del terminal.
	Que no se cuente con un aislamiento del sistema sensible.	Accesos no autorizados a la información mantenida en los sistemas de aplicación.
Gestión de incidentes en la seguridad de la información.	Que no se manejen reportes de eventos en la seguridad de la información.	Que no se tomen medidas correctivas a tiempo, que al no tomarlas puedan afectar a la integridad de la información.
	Que no se designe un responsable de reportar y dar seguimiento a los incidentes de seguridad.	Que se realicen violaciones a la seguridad de la información.
Gestión de la continuidad	Falta de Evaluación de Riesgos	Interrupciones en el desarrollo normal de las

Dominio	Vulnerabilidad	Riesgo
		operaciones de la institución con la pérdida económica que esto conlleva. Que no se mitiguen los riesgos para tratar de reducir el impacto en el caso de que se materialicen.
	Ausencia de un plan de continuidad del negocio que incluya seguridad de la información.	Quiebra de la institución en el caso de que sufra de un desastre natural o provocado. Interrupción de las operaciones, con la pérdida económica correspondiente.
	Que no exista un marco referencial para la planeación de la continuidad del negocio.	Que el plan de continuidad no sea consistente ni aplicado efectivamente identificando prioridades.
	Falta de pruebas del plan de continuidad del negocio.	Que el plan de continuidad no sea aplicado efectivamente cuando ocurra la contingencia.

Tabla 3.4.: Evaluación de Riesgos

3.3. OBJETIVOS

3.3.1. OBJETIVO GENERAL

Auditar la existencia y verificar el cumplimiento de la aplicación, en caso de existir, de las políticas y los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de la información que maneja la Sociedad Financiera con el fin de detectar las oportunidades de mejora que permitirán fortalecer la seguridad de la información en la financiera.

3.3.2. OBJETIVOS ESPECÍFICOS

- Determinar y verificar su cumplimiento, si existieran, de políticas de seguridad que protejan al activo "información" resguardándolo frente a pérdidas.
- Determinar si la información crítica de la institución en términos de disponibilidad, integridad y confidencialidad está expuesta y altamente en riesgo.
- Evaluar la calidad del acceso lógico y físico y los controles de seguridad del ambiente informático.
- Detectar las oportunidades de mejora con respecto a la seguridad de la información.
- Fomentar la conciencia de seguridad a nivel institucional.

3.4. ALCANCE

Al final de este trabajo de auditoría la institución obtendrá:

- Plan y programa de auditoría a la Seguridad de la Información.
- Informe de Auditoría a la Seguridad de la información basada en los controles de la norma ISO 27002:2005 con las oportunidades de mejora y recomendaciones pertinentes.
- Exposición detallada con los puntos relevantes de la auditoría.

3.5. COMPONENTES A AUDITAR

Se evaluarán los siguientes componentes:

Componentes
Política de Seguridad
Organización de la Seguridad de la información
Gestión de Activos
Seguridad de los Recursos Humanos
Seguridad Física y Ambiental
Gestión de las comunicaciones y operaciones
Control de accesos y Gestión de incidentes en la Seguridad de la información
Gestión de la continuidad comercial

Tabla 3.5.: Componentes a auditar

3.6. CRONOGRAMA DE TRABAJO

Para ejecutar la presente auditoría se ha planificado el siguiente cronograma de trabajo:

Actividad	Tiempo
Visita preliminar	2 días
Evaluación de los siguientes componentes:	
Política de Seguridad	2 días
Organización de la Seguridad de la información	7 días
Gestión de Activos	2 días
Seguridad de los Recursos Humanos	1 día
Seguridad física y ambiental	2 días
Gestión de las comunicaciones y operaciones	3 días
Control de accesos y gestión de incidentes en la Seguridad de la información	4 días
Gestión de la continuidad comercial	3 días
Pre-informe	3 días
Elaboración del informe final	3 días
TOTAL:	32 días

Tabla 3.6.: Cronograma de trabajo

3.7. CRITERIOS DE AUDITORÍA A UTILIZARSE

Para realizar la presente auditoría se han tomado como referencia los controles establecidos en la norma ISO 27002:2005, al ser uno de los modelos reconocido internacionalmente.

3.8. RECURSOS DE PERSONAL

Para la presente auditoría participará 1 Auditor Informático y se requiere de la colaboración del Oficial de Seguridad, Auditora Interna y Subgerente de Sistemas de la institución así como del apoyo de la Alta Gerencia, para poder recabar toda la información necesaria.

3.9. HERRAMIENTAS Y TÉCNICAS

Entre las herramientas que se utilizarán para la ejecución de esta auditoría podemos mencionar:

- Norma ISO 27002:2005
- Listas de verificación (check list)
- Correo electrónico
- Computador
- Office (Word, Excel, Power Point)

Adicionalmente se procederá a aplicar las siguientes técnicas a fin de obtener evidencia para poder compararlo con el modelo de mejores prácticas seleccionado (ISO 27002:2005):

- Verbal: Realizando entrevistas al personal involucrado en los temas de seguridad de la información y de los sistemas informáticos en la Financiera.

- Documental: Analizando la Política de Seguridad (si existiera) y evidencia escrita recibida del personal autorizado.

- Física: Observación del cumplimiento de la Política de Seguridad institucional y de los controles de especificados en la norma ISO 27002:2005 referente a los dominios acorde a lo indicado en el alcance definido en esta auditoría.

3.10. PLAN DE COMUNICACIÓN

En la presente auditoría a la seguridad de la información se realizarán, de ser necesario:

- Actas de Reunión firmadas por los involucrados.

- Actas de Entrega / Recepción de los documentos solicitados.

- Informes de Avance de la Auditoría, en caso de ser solicitados por la Gerencia General o Directorio.

- Informe de Auditoría, el cual será expuesto en una reunión final al Directorio y Gerencia General.

Capítulo 4

Ejecución del Programa de Auditoría

4. EJECUCIÓN DEL PROGRAMA DE AUDITORÍA

Durante la fase de ejecución se procedió a revisar los controles de los dominios indicados en la fase de planificación tratando de adaptarlos a las necesidades del negocio y tamaño de la institución. Esto se pudo recabar a través de entrevistas con el Subgerente de Sistemas así como verificaciones in situ en el Centro de Cómputo, haciendo uso de un check list basado en los controles determinados en la norma ISO 27002:2005.

4.1. RIESGOS Y ACCIONES MITIGANTES

A continuación se presentan los riesgos detectados en el capítulo anterior y las acciones mitigantes implementadas por la Sociedad Financiera.

Dominio	Vulnerabilidad	Riesgo	Mitigante(s)
Política de Seguridad	Que falte compromiso por parte de la Alta Gerencia en apoyar al mantenimiento y cumplimiento de la política de Seguridad.	Que la aplicación de la política no sea adecuada, lo cual puede comprometer la integridad, confidencialidad y disponibilidad de la información.	La política de seguridad se encuentra aprobada por la Alta Gerencia y es conocida por el personal. Existe presupuesto del área de Sistemas en el que se incluye inversión en temas de seguridad.
	Que no esté definido un proceso disciplinario (sanciones) por violaciones a las políticas de	Que se violen las políticas de Seguridad al saber que no existe formalmente una sanción.	**No existe.**

Dominio	Vulnerabilidad	Riesgo	Mitigante(s)
	seguridad.		
Organización de la Seguridad de la información	Que los temas de seguridad sean de responsabilidad exclusiva del Área de Sistemas.	Que la aplicación de las políticas de seguridad no sean efectivas.	Revisiones periódicas a los accesos de Usuarios por parte de un área independiente al Área de Sistemas. Auditoría Interna al Departamento de Sistemas. Auditorías externas periódicas.
	Que no estén definidas las responsabilidades del Oficial de Seguridad.	Que no exista responsabilidad en los Controles de Seguridad de la información. Que no se cumplan las políticas de seguridad poniendo en riesgo los criterios de información de disponibilidad, integridad y confidencialidad.	**No existe formalmente definido el perfil del cargo del Oficial de Seguridad.**
	Que no existan procedimientos para cambio de equipos.	Pérdida de la confidencialidad de la información.	**No existe el procedimiento para cambio de equipos.**
Gestión de Activos	Que no se cuente con un inventario de activos que permita identificar sus características y responsables de los mismos.	Pérdida de equipos y de la información contenida en los mismos, poniendo en riesgo la confidencialidad de la información.	Se dispone de un inventario de activos actualizado.
	Que la información no se encuentre correctamente etiquetada e identificada.	Pérdida de la confidencialidad de la información.	**No existe procedimiento para etiquetado e identificación de la información.**
Seguridad de los recursos humanos	Que las funciones y responsabilidades	Accesos no autorizados. Robo, fraude o mal	Existen procedimientos formales para la

Dominio	Vulnerabilidad	Riesgo	Mitigante(s)
	del personal no se encuentren definidas (roles y perfiles de usuario).	uso de la información a su cargo. Pérdida de la confidencialidad e integridad de la información. Imposibilidad de detectar oportunamente posibles violaciones de seguridad.	creación de usuarios y permisos de acceso.
	Falta de capacitación en temas de Seguridad de la Información.	Error humano por falta de conocimiento que puede afectar a la integridad o confidencialidad de la información.	**No existe capacitación en temas referentes a la Seguridad de la Información.**
Seguridad física	Inexistencia de controles de entrada físicos al Centro de Cómputo.	Accesos no autorizados que puedan ocasionar de forma intencionada o no, alteraciones en las actividades normales de procesamiento o extracción de información sensitiva para la institución.	Existe cerradura eléctrica y un gabinete de servidores que se encuentra bajo llave.
	Falta de protección física contra daños ambientales o creados por el hombre.	Pérdidas o daños irreparables en los recursos de información al presentarse desastres y no estar preparados, con lo cual se puede poner en riesgo la disponibilidad de la información.	Existe extintor de incendio, detector de humo, acondicionador de aire exclusivo para el área de servidores (adicional a la central de aire).
	Falta de procedimientos	Accesos no autorizados.	**No Existe procedimiento para**

Dominio	Vulnerabilidad	Riesgo	Mitigante(s)
	para manejo de equipos fuera de la institución.		**manejo de equipos fuera de la institución.**
	Falta de procedimientos para la eliminación segura de equipos.	Pérdida de la confidencialidad de la información.	**No existe procedimiento para eliminación segura de equipos.**
	Que no existan autorizaciones para trasladar equipos.	Accesos no autorizados y pérdida de la confidencialidad de la información.	Se manejan autorizaciones para trasladar equipos fuera de la organización.
Gestión de las comunicaciones y operaciones	Que no se cuente con la suficiente documentación relativa a los procedimientos de operación.	No ejecución de procesos claves que afecten a la integridad y disponibilidad de la información.	Los principales procedimientos de operación se encuentran documentados.
	Que no exista un procedimiento formal de control de cambios en los sistemas informáticos.	Ejecución de programas sin autorización que afecten a la integridad y disponibilidad de la información.	Existe un procedimiento formal de control de cambios en los sistemas informáticos (autorizaciones formales).
	Inadecuada segregación de funciones.	Robo, fraude o mal uso de la información a su cargo. Imposibilidad de detectar oportunamente posibles violaciones de seguridad.	Se realizan auditorías externas (trimestralmente) y auditorías internas durante el año.
	Que no se encuentren separados los ambientes de desarrollo y producción.	Accesos y ejecución de programas no autorizados.	Existe un servidor de producción y un servidor de desarrollo.
	Que no existan controles de seguridad,	Que no se cuente con los equipos o servicios necesarios	La compañía cuenta con un Dpto. Legal el cual revisa

Dominio	Vulnerabilidad	Riesgo	Mitigante(s)
	definiciones de servicio y niveles de entrega incluidos en contratos de terceros.	para el desarrollo normal de las operaciones lo que puede afectar a la integridad y disponibilidad de la información.	minuciosamente los contratos con terceros.
	Que no se realicen monitoreos a la capacidad de los recursos.	Fallas en los sistemas o equipos que afectan a la disponibilidad e integridad de la información.	Se realizan monitoreos de capacidad de disco duro del servidor de producción.
	Que no existan controles contra software malicioso (Virus)	Pérdida de la integridad y disponibilidad en los sistemas y en la información.	Se cuenta con un antivirus corporativo (NOD32).
	Que no se realicen respaldos de la información y software esencial.	Pérdida de la integridad y disponibilidad en los sistemas y en la información, pudiendo poner en riesgo la continuidad del negocio.	Se realizan respaldos periódicos de la base de datos principal (Oracle) 2 veces al día y diariamente se respalda el software esencial.
	Que no existan procedimientos para la gestión de medios removibles.	Pérdida de la confidencialidad de la información almacenada en medios removibles.	**No existe procedimiento para la gestión de medios removibles.**
	Que no existan procedimientos para la eliminación de medios removibles.	Pérdida de la confidencialidad de la información almacenada en medios removibles.	**No existe procedimiento para la eliminación de medios removibles.**
	Que no existan controles para proteger la documentación del sistema.	Divulgación no autorizada que afecta a la confidencialidad de la información.	La documentación del sistema está a cargo exclusivamente del personal del área de Sistemas.
	Ausencia de logs de auditoría.	Imposibilidad de detectar oportunamente	Se pudo evidenciar la existencia de logs de auditoría a nivel de los

Dominio	Vulnerabilidad	Riesgo	Mitigante(s)
		posibles violaciones de seguridad.	sistemas de Cartera, Contabilidad y Depósitos a Plazo.
	Ausencia de bitácoras de operaciones	Imposibilidad detectar oportunamente posibles actividades de procesamiento de información no autorizadas.	Existe una bitácora de las actividades realizadas diariamente por el personal del área.
Control de acceso	Ausencia de un procedimiento para el registro de nuevos usuarios y asignación de privilegios.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.	Existen procedimientos para la creación de usuarios y accesos a las diferentes opciones de los sistemas.
	Que no exista un procedimiento formal para la asignación de claves.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.	**No existe un procedimiento formal para la asignación de claves.**
	Que no se revisen los derechos de acceso de los usuarios utilizando un proceso formal.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.	Los derechos de acceso son revisados periódicamente por el área de Auditoría y comunicados a través de informes formales a la Alta Gerencia.
	Que no existan buenas prácticas en el uso de claves.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.	Existen políticas que definen las características de las claves (mayúsculas, minúsculas, números y que no sean igual al login de usuario), tampoco se puede repetir las 10 últimas claves utilizadas.
	Que no exista protección al equipo desatendido.	Accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.	Los equipos se bloquean con contraseña luego de 10 minutos de inactividad.
	Que no se cuente	Accesos no	**No existe una política**

Dominio	Vulnerabilidad	Riesgo	Mitigante(s)
	con una política de pantalla y escritorio limpios.	autorizados que pueden afectar a la confidencialidad e integridad de la información.	**de pantalla y escritorio limpios.**
	Que no exista autenticación de usuario en el terminal.	Accesos no autorizados al Sistema Operativo del terminal.	Todos los usuarios se autentifican al encender sus computadores a través de un servidor de dominio (Windows Server 2003).
	Que las sesiones de usuario queden activas luego de un largo periodo de inactividad.	Accesos no autorizados al Sistema Operativo del terminal.	**Las sesiones de usuario no se cierran automáticamente luego de un tiempo de inactividad en las diferentes aplicaciones.**
	Que no se cuente con un aislamiento del sistema sensible.	Accesos no autorizados a la información mantenida en los sistemas de aplicación.	El sistema se encuentra aislado en un ambiente exclusivo.
Gestión de incidentes en la seguridad de la información.	Que no se manejen reportes de eventos en la seguridad de la información.	Que no se tomen medidas correctivas a tiempo, que al no tomarlas puedan afectar a la integridad de la información.	**No existen reportes de eventos que afectan a la seguridad de la información.**
	Que no se designe un responsable de reportar y dar seguimiento a los incidentes de seguridad.	Que se realicen violaciones a la seguridad de la información.	**No existe un responsable de reportar y dar seguimiento a los incidentes de seguridad.**
Gestión de la continuidad	Falta de Evaluación de Riesgos	Interrupciones en el desarrollo normal de las operaciones de la institución con la pérdida económica que esto conlleva.	El área de Riesgos es la encargada de realizar la Gestión de Riesgos de la compañía.

Dominio	Vulnerabilidad	Riesgo	Mitigante(s)
		Que no se mitiguen los riesgos para tratar de reducir el impacto en el caso de que se materialicen.	
	Ausencia de un plan de continuidad del negocio que incluya seguridad de la información.	Quiebra de la institución en el caso de que sufra de un desastre natural o provocado. Interrupción de las operaciones, con la pérdida económica correspondiente.	Existe un plan de contingencias y continuidad del negocio el cual incluye: Análisis de Impacto del negocio, procedimientos de recuperación de las Bases de Datos y aplicaciones críticas, política de mantenimiento y el resultado de la última prueba realizada.
	Que no exista un marco referencial para la planeación de la continuidad del negocio.	Que el plan de continuidad no sea consistente ni aplicado efectivamente identificando prioridades.	**No existe un marco referencial para la planeación de la continuidad del negocio.**
	Falta de pruebas del plan de continuidad del negocio.	Que el plan de continuidad no sea aplicado efectivamente cuando ocurra la contingencia.	Existe un resumen del resultado de la última prueba realizada.

Tabla 4.1.: Evaluación de Riesgos y mitigantes

4.2. HALLAZGOS DE MAYOR IMPORTANCIA DETECTADOS EN LA EJECUCIÓN DE LA AUDITORÍA

Al evaluar los procedimientos mitigantes implementados por la institución de acuerdo a su política de seguridad y referenciando los controles definidos en la norma ISO 27002:2005, se presenta la cédula de los hallazgos de mayor relevancia por cada uno de los dominios de acuerdo a las características y necesidades del negocio.

4.2.1. POLÍTICA DE SEGURIDAD

Cédula del Hallazgo No.:	01
Fecha:	13/06/2011
Dominio:	Política de Seguridad
Control:	Política de Seguridad aprobada por el Directorio
Criterio: "Cualquier software a instalarse deberá ser realizado por el departamento de sistemas, el cual se asegurará que provenga de fuentes conocidas y seguras, además de cerciorarse de que dicha instalación no cree conflicto alguno".	
Causa: Los usuarios tienen perfil "Administrador" en el computador por lo cual pueden instalar cualquier tipo de software.	
Efecto: Afectar al rendimiento del computador del usuario así como también se pueden producir filtraciones de código malicioso de software no autorizado que pueden poner en riesgo la disponibilidad e integridad de la información, además del riesgo legal asociado al tener instalado software sin licencias autorizadas que puede crear demandas o problemas legales entre la institución y los propietarios de software.	
Conclusión: No se controla la aplicación de la política de seguridad referente a la instalación de software autorizado.	
Recomendación: Cambiar el perfil de los usuarios con un perfil de privilegios limitados a fin de evitar la instalación de software no autorizado.	

Cédula del Hallazgo No.:	02
Fecha:	13/06/2011
Dominio:	Política de Seguridad
Control:	Política de Seguridad aprobada por el Directorio
Criterio: "Sistemas actualizará en forma permanente los últimos parches de seguridad de las estaciones de trabajo."	
Causa: No existe un registro de las últimas actualizaciones (parches de seguridad) instaladas en los equipos de los usuarios.	
Efecto: Las aplicaciones podrían dejar de funcionar correctamente poniendo en riesgo la operatividad de los sistemas.	
Conclusión: No se lleva un control de las actualizaciones (parches de seguridad).	
Recomendación: Llevar un control, en lo posible que sea automático, de las actualizaciones (parches de seguridad) y crear el procedimiento respectivo que incluya: periodicidad, responsable y pruebas realizadas con la actualización que certifiquen que no afectan a la ejecución de los aplicativos.	

Cédula del Hallazgo No.:	03
Fecha:	13/06/2011
Dominio:	Política de Seguridad
Control:	Política de Seguridad aprobada por el Directorio
Criterio: Política de Seguridad actualizada.	
Causa: La política de seguridad no se encuentra actualizada.	
Efecto: En el documento de Políticas de Seguridad se menciona el Software "Norton Antivirus", sin embargo, éste no es el sistema Antivirus que posee la empresa, lo cual podría afectar a la aplicación de la política de seguridad referente a la protección de equipos a través del antivirus "NOD32" que es el que realmente tiene implementado.	
Conclusión: La política de seguridad no se encuentra actualizada o no ha sido correctamente revisada.	
Recomendación: La Alta Gerencia deberá disponer que el área de Auditoría realice revisiones periódicas a la política de seguridad cada vez que se realicen cambios significativos en la tecnología o en los procedimientos del área de Sistemas así como revisiones que permitan verificar el cumplimiento de la política; además de procurar en lo posible no incluir nombres comerciales de aplicaciones ya que la política de seguridad debe ser una directriz general para una adecuada administración de la Seguridad de la información de la compañía.	

Cédula del Hallazgo No.:	04
Fecha:	14/06/2011
Dominio:	Política de Seguridad
Control:	Política de Seguridad aprobada por el Directorio
Criterio: "Escaneo automático de Virus en el computador del usuario, los viernes a las 17h00".	
Causa: No se encuentra programada la ejecución automática del Antivirus en los computadores de los usuarios.	
Efecto: Computadores infectados lo cual puede afectar a la disponibilidad del equipo, provocando interrupciones en el trabajo del usuario e incluso pérdida de información afectando la integridad de la información.	
Conclusión: La política no posee el control para que se cumpla la ejecución automática del antivirus en los computadores de los usuarios lo cual denota una falta de control interno que permita verificar el cumplimiento de la política de seguridad.	
Recomendación: La Alta Gerencia deberá disponer al área de Auditoría que incluya en su programa anual la revisión periódica del cumplimiento de la política de seguridad verificando la correcta implementación de los controles necesarios para su aplicabilidad.	

Cédula del Hallazgo No.:	05
Fecha:	14/06/2011
Dominio:	Política de Seguridad
Control:	Política de Seguridad aprobada por el Directorio
Criterio: "Para realizar cualquier ingerencia en la base de datos de producción por parte del DBA, se deberá solicitar por escrito la autorización al oficial de seguridad de la información".	
Causa: No se pudo evidenciar la existencia de solicitudes formales al Oficial de Seguridad para realizar cambios a la Base de Datos de producción. Se pudo evidenciar que existen "reversiones" que se realizan de manera manual por parte del DBA como: Anulación del "Comprobante de Ingreso" (emitido en Caja) Anulación de "Liquidación de Crédito" (emitido por Oficial de Crédito)	
Efecto: Modificaciones no autorizadas ni controladas que pueden afectar a la integridad de la información que se encuentra en el almacén de datos principal con los riesgos inherentes a este tipo de acciones.	
Conclusión: No se está cumpliendo la política referente a cambios en la Base de Datos de producción lo cual puede afectar a la integridad y disponibilidad de la información.	
Recomendación: Que no se realicen modificaciones directas a la base de datos y que se desarrollen opciones en el Sistema que permitan realizar este tipo de reversiones o anulaciones manteniendo las respectivas pistas de auditoría para su posterior revisión y que estas funciones operativas sean asignadas a personal de las áreas usuarias de acuerdo a sus perfiles de usuario contando siempre con las autorizaciones de alto nivel necesarias para este tipo de acciones las mismas que deben estar formalmente establecidas en las políticas y procedimientos de la compañía.	

Cédula del Hallazgo No.:	06
Fecha:	14/06/2011
Dominio:	Política de Seguridad
Control:	Política de Seguridad aprobada por el Directorio
Criterio: Pistas de Auditoría y control de acceso a la Base de Datos de producción.	
Causa: El DBA utiliza el usuario genérico "system" para acceder a la Base de Datos principal (Oracle) y no se encuentran levantadas las pistas de auditoría de la Base de Datos Oracle por lo que no se deja evidencia de las modificaciones que puede realizar el DBA en la Base de Datos de producción.	
Efecto: Modificaciones no autorizadas ni controladas que pueden afectar a la integridad de la información que se encuentra en el almacén de datos principal con los riesgos inherentes a este tipo de acciones.	
Conclusión: No se puede definir la responsabilidad de los cambios realizados en la Base de Datos ya que se está utilizando un usuario genérico y no se encuentran levantadas las pistas de auditoría lo cual puede afectar a la integridad y confidencialidad de la información de los datos.	
Recomendación: Que se cree un usuario personal para ser utilizado por el DBA y se desactiven los usuarios genéricos que tenga la Base de Datos principal, además las pistas de auditoría de la Base de Datos deben ser activadas y revisadas periódicamente a través de un proceso formal por el área de Auditoría e informar a la Alta Gerencia el resultado de estas revisiones.	

4.2.2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Cédula del Hallazgo No.:	07
Fecha:	17/06/2011
Dominio:	Aspectos organizativos de la Seguridad de la Información
Control:	Perfil del Cargo del Oficial de Seguridad
Criterio: Tener definidas las funciones y responsabilidades del Oficial de Seguridad.	
Causa: No se encuentran definidas las funciones y responsabilidades del Oficial de Seguridad. El cargo ha sido asignado al Auditor Interno en lo referente a la custodia de las claves de los servidores y base de datos principal, transportación de los respaldos a una ubicación externa, revisión de los logs de auditoría y accesos otorgados a los usuarios e informe de estas revisiones a la Alta Gerencia. El Subgerente de Sistemas es quien maneja los temas de Seguridad de la Información en lo que se refiere a la parte tecnológica y asignación de accesos a los usuarios, teniendo él también acceso a los diferentes sistemas a manera de súper usuario.	
Efecto: Que los temas relacionados a la Seguridad de la Información no sean tratados con la debida diligencia, compromiso y de manera efectiva. La Administración de Usuarios está siendo manejada por el Área de Sistemas lo cual puede provocar conflictos de intereses y accesos no autorizados que pueden afectar a la confidencialidad e integridad de la información.	
Conclusión: No se puede definir la responsabilidad del Oficial de Seguridad en los diferentes procesos en los que pueda intervenir.	
Recomendación: Que se defina y se apruebe formalmente el perfil del cargo del Oficial de Seguridad el cual debe pertenecer a un área independiente al Área de Sistemas, reportar a la Alta Dirección y en lo posible no ser usuario operativo de las aplicaciones a fin de evitar conflictos de intereses a través de la segregación de funciones.	

4.2.3. GESTIÓN DE ACTIVOS

Cédula del Hallazgo No.:	08
Fecha:	21/06/2011
Dominio:	Gestión de Activos
Control:	Clasificación y etiquetado de la información
Criterio: Política para la clasificación y etiquetado de la información.	
Causa: No existen políticas ni procedimientos para la clasificación y etiquetado de la información.	
Efecto: Accesos no autorizados a la información ya sea esta digital o física, lo cual puede provocar pérdida de la confidencialidad de la información.	
Conclusión: La información no se encuentra debidamente clasificada y etiquetada lo cual puede provocar pérdida de la confidencialidad de la información.	
Recomendación: Que se defina una política y procedimientos necesarios para una adecuada clasificación y etiquetado de la información así como de "escritorio limpio" (sin información confidencial a la vista) y capacitación a los usuarios para el correcto uso de la información confidencial y de uso interno acorde a las necesidades de la compañía.	

4.2.4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Cédula del Hallazgo No.:	09
Fecha:	22/06/2011
Dominio:	Seguridad ligada a los recursos humanos
Control:	Proceso disciplinario
Criterio: Que exista un proceso disciplinario formal para los empleados que han comprometido una vulnerabilidad de seguridad.	
Causa: No existe un proceso disciplinario en casos de violaciones a las políticas de seguridad por parte de los empleados.	
Efecto: Incumplimiento a las políticas de seguridad sin poder sancionar a los responsables.	
Conclusión: Al no existir un proceso disciplinario, no se puede sancionar a los empleados que violen las políticas de seguridad comprometiendo la integridad, confidencialidad y disponibilidad de la información.	
Recomendación: Que se incluya en la política de seguridad un proceso disciplinario para los empleados que violen la política de seguridad y que éstas sean difundidas a todo el personal a través de concienciación y capacitación continua así como revisiones independientes y periódicas para verificar el cumplimiento de la política y el respectivo reporte a la Alta Gerencia.	

4.2.5. SEGURIDAD FÍSICA Y AMBIENTAL

Cédula del Hallazgo No.:	10
Fecha:	23/06/2011
Dominio:	Seguridad Física y Ambiental
Control:	Mantenimiento de equipos
Criterio: Plan de mantenimiento de equipos de usuarios.	
Causa: En el cronograma del Departamento de Sistemas no se evidencian actividades relacionadas al mantenimiento de equipos de los usuarios.	
Efecto: Daños inesperados en los computadores o servidores que pueden afectar a la disponibilidad e integridad de la información y a la continuidad de los procesos normales del negocio.	
Conclusión: No se puede garantizar el normal funcionamiento de los equipos al no realizarse los mantenimientos preventivos a los mismos.	
Recomendación: Que se establezca un plan de mantenimiento de los equipos de la institución que garanticen la disponibilidad de los equipos y la continuidad de las operaciones normales de la institución.	

Cédula del Hallazgo No.:	11
Fecha:	23/06/2011
Dominio:	Seguridad Física y Ambiental
Control:	Protección y aislamiento de los equipos
Criterio: Los equipos se aíslan o se protegen para reducir los riesgos de las amenazas y peligros medioambientales y para reducir las oportunidades de acceso no autorizado.	
Causa: Los servidores se encuentran ubicados en un gabinete cerrado dentro del área de Sistemas la cual está separada por paredes falsas de madera, tela y aluminio y contigua a un área de archivos, sin embargo, si cuenta con extintor de incendio, detectores de humo, control de temperatura y humedad, sensores de movimiento, cerradura eléctrica, entre otros.	
Efecto: Fácil propagación del calor en caso de un siniestro al estar junto a un área en el que se guarda material de fácil combustión, lo cual puede comprometer la disponibilidad de los servicios de TI y la continuidad del negocio.	
Conclusión: El área de servidores no se encuentra totalmente protegida y se encuentra junto a un área que almacena material de fácil combustión.	
Recomendación: Que se aísle de mejor manera los servidores en un área de difícil acceso, si es posible fuera del Área de Sistemas y que no esté expuesto a los riesgos medioambientales a través de la implementación de un centro de cómputo que cumpla con todos los estándares de seguridad con normas que permitan su adecuada protección y alejado de áreas que almacenen materiales de fácil combustión.	

Cédula del Hallazgo No.:	12
Fecha:	23/06/2011
Dominio:	Seguridad Física y Ambiental
Control:	Seguridad en el cableado
Criterio: El cableado de energía eléctrica está protegido para evitar daños.	
Causa: En el área de TI, que es dónde se encuentran los servidores, se pudo evidenciar la existencia de una conexión que termina en un breker al cual llegan cables de luz que no están protegidos.	
Efecto: En caso de un cortocircuito, al tener un cableado eléctrico que no está totalmente protegido, puede provocar un siniestro mayor que puede afectar a la disponibilidad de la información y continuidad de las operaciones normales del negocio.	
Conclusión: El área de servidores se encuentra expuesta a daños provocados por el cableado que no está protegido.	

Recomendación:
Que se realicen las adecuaciones necesarias para proteger el cableado de energía eléctrica que llega al breker, con el fin de evitar siniestros. (Ver recomendación anterior).

Cédula del Hallazgo No.:	13
Fecha:	23/06/2011
Dominio:	Seguridad Física y Ambiental
Control:	Reutilización o eliminación segura de equipos
Criterio: Los equipos destinados a eliminación o reutilización, que contienen disco, se verifican previamente asegurando que toda la información delicada o el software licenciado se destruyen físicamente, o son sobrescritos de manera segura.	
Causa: No existe un procedimiento formal de eliminación de equipos y se pudo evidenciar que existen computadores que mantienen el nombre del computador identificado por el área a la que pertenecieron anteriormente, lo que evidencia que no se ha aplicado un procedimiento para la reutilización de los mismos.	
Efecto: Accesos no autorizados a la información con la pérdida de confidencialidad que esto conlleva.	
Conclusión: No se puede garantizar que cuando los equipos son reutilizados o eliminados, exista información sensible que puede llegar a terceros no autorizados.	
Recomendación: Establecer procedimientos para la eliminación o reutilización de los equipos y un área o función que permita la verificación de estos procedimientos a fin de garantizar la adecuada aplicación de los mismos (control de calidad).	

4.2.6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

Cédula del Hallazgo No.:	14
Fecha:	24/06/2011
Dominio:	Gestión de las comunicaciones y operaciones
Control:	Respaldos (back-up)
Criterio: Se deben realizar respaldos de la información comercial y software esencial.	
Causa: En el procedimiento de Respaldos diarios de la Base de Datos principal se indica que "el Auditor Interno firma la bitácora de respaldos de base de datos para dejar constancia de que le han entregado el respaldo", sin embargo, no existe evidencia de la entrega del respaldo al Auditor Interno. Los respaldos de los usuarios, así como las bases de datos de los aplicativos "satélites" (Nómina, Recursos Humanos, Proveeduría, Activos Fijos, Depósitos a Plazo que utilizan otras bases de datos y que se integran al Sistema principal a través de interfases) no se almacenan en un lugar externo a la institución.	
Efecto: Que no se pueda garantizar la continuidad de las operaciones en el caso de que suceda un siniestro y no se cuente con el último respaldo tanto de la base de datos Oracle como de las demás aplicaciones en una ubicación externa.	
Conclusión: No se está cumpliendo totalmente el procedimiento de Respaldos y no se está respaldando toda la información de los usuarios y aplicaciones "satélites" en un lugar externo.	
Recomendación: La Alta Gerencia deberá analizar la factibilidad de que los respaldos sean enviados al casillero de seguridad a través de un tercero al ser información del negocio sensible y confidencial de tal forma que se garantice la responsabilidad de llevar los mismos a la ubicación externa; el área de Auditoría es la responsable del control interno verificando que el procedimiento de respaldo se cumpla con la periodicidad e información definida y no debería tener la responsabilidad del traslado de los respaldos pues entraría en conflicto de intereses por una inadecuada segregación de funciones. Los respaldos de los usuarios y de las bases de datos de los aplicativos "satélites" también deben almacenarse en una ubicación externa en la periodicidad que determine la Alta Gerencia de acuerdo a las necesidades de la institución.	

Cédula del Hallazgo No.:	15
Fecha:	24/06/2011
Dominio:	Gestión de las comunicaciones y operaciones
Control:	Segregación de deberes
Criterio: Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no autorizada o no intencionada o un mal uso de los activos de la organización.	
Causa: Se pudo evidenciar que el Asistente de Sistemas es quien realiza las pruebas y pasos a producción de los cambios por él desarrollados, según la firma del "Formulario de Control de Versiones de Software".	
Efecto: Modificaciones no autorizadas o mal intencionadas que pueden afectar a la integridad o disponibilidad de la información que se encuentra en las bases de datos así como a la materialización de un fraude interno.	
Conclusión: El procedimiento de "Desarrollo de Software", en la fase de "Pruebas" indica que es el Asistente de Sistemas quien realiza las pruebas con el usuario, lo cual hace que se cree conflicto de intereses por la falta de segregación de funciones.	
Recomendación: Modificar el procedimiento de "Desarrollo de Software" en la fase de "Pruebas", asignando esta tarea así como los pases a producción a otra persona (Ej. Personal del Área de Seguridad u otra función independiente al desarrollador) a fin de segregar las funciones incompatibles ya que actualmente lo hace la misma persona que desarrolló el cambio.	

Cédula del Hallazgo No.:	16
Fecha:	27/06/2011
Dominio:	Gestión de las comunicaciones y operaciones
Control:	Aceptación del Sistema
Criterio: Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas de los sistemas durante su desarrollo y antes de su aceptación.	
Causa: No se pudo evidenciar la existencia de un plan de pruebas para los cambios que se realizan en los sistemas; existe el "Formulario de Control de Versiones de Software" en el cual solo se menciona que se han realizado las pruebas con el usuario y su aceptación, pero no se indican qué pruebas fueron realizadas.	
Efecto: Modificaciones no autorizadas o mal intencionadas que pueden afectar a la integridad o disponibilidad de la información que se encuentra en las bases de datos.	
Conclusión: El procedimiento de "Desarrollo de Software", en la fase de "Pruebas" no indica qué tipo de pruebas y la forma de documentar las mismas.	
Recomendación: Modificar el procedimiento de "Desarrollo de Software" en la fase de "Pruebas" indicando: Procedimiento del Plan de pruebas, formulario requerido para dejar evidencia de la realización de las mismas, lista de verificación con las pruebas mínimas que deben ser realizadas y que estas pruebas las realice una persona diferente a la que desarrolló el cambio.	

4.2.7. CONTROL DE ACCESOS

Cédula del Hallazgo No.:	17
Fecha:	28/06/2011
Dominio:	Control de Accesos
Control:	Gestión del acceso del usuario
Criterio: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.	
Causa: Se pudo evidenciar que es el Subgerente de Sistemas quien registra los usuarios y otorga los permisos de acceso a las diferentes opciones, también teniendo él acceso a las diferentes aplicaciones en producción.	
Efecto: Se pueden dar accesos no autorizados por parte del Subgerente de Sistemas, crear súper usuarios y al tener también acceso directo a las diferentes tablas del sistema, puede afectar a la integridad, confiabilidad y confidencialidad de la información y el riesgo de posibles fraudes internos.	
Conclusión: El procedimiento no garantiza una correcta gestión del acceso del usuario lo cual denota un alto riesgo operativo que puede provocar accesos no autorizados, fraudes internos y falta de integridad, confiabilidad y confidencialidad de la información.	
Recomendación: Asignar la responsabilidad de la gestión de usuarios al Oficial de Seguridad así como de revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal y reportar a la Alta Gerencia.	

Cédula del Hallazgo No.:	18
Fecha:	28/06/2011
Dominio:	Control de Accesos
Control:	Gestión del acceso del usuario
Criterio: La asignación de claves se debe controlar a través de un proceso de gestión formal.	
Causa: No existe un procedimiento formal de entrega/recepción de las claves de usuario.	
Efecto: Se pueden crear accesos no autorizados que afecten a la integridad y confidencialidad de la información.	
Conclusión: El procedimiento no garantiza una correcta gestión en la entrega de claves.	
Recomendación: Crear el procedimiento formal para entrega de contraseñas, dejando un registro de la entrega/recepción de la clave y la responsabilidad sobre la misma.	

Cédula del Hallazgo No.:	19
Fecha:	29/06/2011
Dominio:	Control de Accesos
Control:	Control de acceso a redes
Criterio: Evitar el acceso no autorizado a los servicios en red.	
Causa: No existe un procedimiento formal de monitoreo de la red de computadoras en la institución.	
Efecto: Se pueden crear accesos no autorizados que afecten a la integridad y confidencialidad de la información.	
Conclusión: Al no realizarse los monitoreos de la red, se pueden crear accesos no autorizados que afecten a la confidencialidad, integridad y disponibilidad de los servicios informáticos.	
Recomendación: Crear el procedimiento formal y los controles necesarios para realizar monitoreos periódicos de la red de computadoras y sus respectivos informes a la Alta Gerencia a fin de dar seguimiento y solución a los incidentes de red identificados.	

Cédula del Hallazgo No.:	20
Fecha:	29/06/2011
Dominio:	Control de Accesos
Control:	Sesión inactiva.
Criterio: Evitar accesos no autorizados a los sistemas críticos.	
Causa: El Sistema de Cartera y Contabilidad no posee el control para cerrar automáticamente una sesión inactiva.	
Efecto: Se pueden provocar accesos no autorizados que afecten a la integridad y confidencialidad de la información.	
Conclusión: Al no cerrar automáticamente las sesiones inactivas se corre el riesgo de que se produzcan accesos no autorizados a los aplicativos críticos de la institución.	
Recomendación: Desarrollar en el Sistema de Cartera y Contabilidad la rutina para cerrar la aplicación luego de un tiempo determinado de inactividad en el mismo.	

4.2.8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Cédula del Hallazgo No.:	21
Fecha:	29/06/2011
Dominio:	Gestión de incidentes en la seguridad de la información
Control:	Reporte de eventos en la seguridad de la información
Criterio: Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.	
Causa: No existe un procedimiento formal que asegure el reporte a la Alta Gerencia de los incidentes que puedan poner en riesgo la seguridad de la información.	
Efecto: Que se produzcan incidentes de seguridad que pueden afectar a la integridad, confidencialidad y disponibilidad de la información.	
Conclusión: Al no existir un procedimiento para reportar los incidentes de seguridad, no se pueden tomar las medidas correctivas necesarias.	
Recomendación: Crear políticas y procedimientos formales para la gestión de incidentes, así como la asignación de la responsabilidad de reportarlos a la Alta Gerencia a fin de tomar medidas correctivas o de mejora. Estos reportes de incidentes deben incluir	

al menos: forma en que inició el incidente, vulnerabilidades explotadas, forma de detección, solución temporal, responsable de la detección del incidente entre otros.

4.2.9. GESTIÓN DE LA CONTINUIDAD COMERCIAL

Cédula del Hallazgo No.:	22
Fecha:	30/06/2011
Dominio:	Gestión de la continuidad comercial
Control:	Marco referencial para la planeación de la continuidad comercial.
Criterio: Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las pruebas y mantenimiento.	
Causa: No existe una metodología o marco referencial formalmente establecido y aprobado que garantice el proceso de Administración de la Continuidad del Negocio. No existe evidencia de la capacitación realizada en los temas relacionados al BCP, tampoco se detallan las actividades a realizar por cada uno de los responsables pues están descritas de manera general. No están definidos los procedimientos y formularios manuales que se van a utilizar cuando ocurra un evento que ponga en riesgo la continuidad de las operaciones, ni las políticas y procedimientos que van a regir durante la contingencia.	
Efecto: Que no se puedan integrar los planes de contingencia departamentales en el momento de una interrupción del negocio. Que la aplicación del plan no sea efectiva afectando la continuidad del negocio.	
Conclusión: Existe un plan de continuidad de negocio estructurado que contiene: Análisis de Impacto del negocio, procedimientos de recuperación de las Bases de Datos y aplicaciones críticas, política de mantenimiento y el resultado de la última prueba realizada. Sin embargo, no todo el personal ha sido capacitado en los procedimientos a realizarse en caso de una contingencia mayor que comprometa la continuidad del negocio, tampoco han sido definidas las políticas y procedimientos que van a regir durante la contingencia, lo cual podría afectar a la ejecución del plan.	
Recomendación: Crear la metodología de la Planeación de la continuidad a fin de alinear los planes departamentales con el plan de continuidad del negocio general que tiene la institución y se pueda crear el proceso de Administración de la Continuidad del negocio. Esta metodología debe incluir al menos los siguientes temas: • Análisis de Impacto del Negocio (que si se lo ha hecho actualmente). • Definición de Estrategias de recuperación.	

- Forma de implantar la estrategia de recuperación y responsables de la misma.
- Plan de Pruebas y mantenimiento del Plan de Continuidad del Negocio.

La Alta Dirección debe estar consciente que la Continuidad del negocio es un proceso que atañe no solamente al área de tecnología sino a toda la institución, el mismo que debe ser retroalimentado a partir de las pruebas realizadas para analizar las brechas a fin de que su aplicación sea efectiva y eficiente.

Se sugiere que el Plan de continuidad del negocio sea actualizado, aprobado y difundido al personal cada vez que se realicen cambios en los colaboradores responsables de la ejecución del mismo o se implementen nuevos procesos críticos; además se debe detallar las actividades y procedimientos a seguir por cada uno de los responsables durante la ejecución del plan. Cabe mencionar que este Plan de continuidad debe respaldarse en un lugar externo a la institución para garantizar su disponibilidad y fácil acceso en caso de una contingencia o siniestro.

Capítulo 5
Resultados

5. RESULTADOS

Una vez revisados los hallazgos encontrados durante la ejecución de la auditoría se puede determinar que la Sociedad Financiera mantiene ciertas debilidades en la administración de la seguridad y aplicación de la Política de Seguridad institucional; se considera la existencia de controles aceptables a nivel de las aplicaciones, gestión de activos, seguridad física, ambiental y de recursos humanos, pero existen debilidades referentes a segregación de funciones, controles de acceso a la base de datos y en la gestión de incidentes, en los cuales se deben implementar los controles necesarios que mitiguen los riesgos de seguridad a los que están expuestos y que pueden comprometer a la integridad, confidencialidad y disponibilidad de la información administrada por la institución financiera.

El criterio utilizado para esta evaluación ha sido el grado de exposición al riesgo en los diferentes dominios revisados en base a los hallazgos encontrados y documentados en el capítulo anterior y utilizando la siguiente escala de evaluación.

Nivel de Riesgo	Descripción
Alto	Los controles internos no bastan para proteger los activos de información o minimizar la exposición a pérdidas en el dominio evaluado.
Medio	La mayor parte de los controles internos implementados son aceptables. No obstante se identificaron algunas oportunidades de mejora que deben ser consideradas y tratadas.
Bajo	Los controles internos funcionan correctamente y cubren la mayor parte de los riesgos identificados en el dominio.

Tabla 5.1.: Escala de Evaluación

A continuación se detalla el nivel de riesgo de acuerdo a los hallazgos identificados para cada dominio evaluado.

Dominio evaluado	Riesgo
Política de Seguridad	**Alto**
Organización de la Seguridad de la información	**Medio**
Gestión de Activos	**Bajo**
Seguridad de los Recursos Humanos	**Bajo**
Seguridad física y ambiental	**Medio**
Gestión de las comunicaciones y operaciones	**Alto**
Control de accesos	**Alto**
Gestión de incidentes en la Seguridad de la información	**Alto**
Gestión de la continuidad comercial	**Medio**

Tabla 5.2.: Resultados de dominios evaluados

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Al realizar esta auditoría a la seguridad de la información se puede concluir que:

1. Utilizar estándares ya establecidos como el modelo de buenas prácticas reconocido ISO 27002:2005 permite razonablemente evaluar en forma estructurada los aspectos de seguridad de la información de una organización.

2. Los temas de Seguridad de la Información son de vital importancia en la administración y buen funcionamiento de una institución financiera regulada.

3. La autoridad y compromiso de la Alta Dirección son un factor clave para facilitar la ejecución y buen término de la auditoría.

4. La institución financiera mantiene una seguridad razonable en sus sistemas de información a nivel de aplicativos informáticos, sin embargo, presenta ciertas oportunidades de mejora relacionadas a la segregación de funciones, controles de acceso a la administración de la base de datos y en la gestión de incidentes.

RECOMENDACIONES

El Informe de Auditoría presentado a la Sociedad Financiera contiene oportunidades de mejora relacionadas a los diferentes dominios evaluados de acuerdo a los controles de la norma ISO 27002:2005, por lo que se recomienda que:

1. La Alta Gerencia comprometa al personal de las áreas involucradas y entregue todo el apoyo necesario a fin de cumplir las recomendaciones indicadas en el informe.

2. Desarrollar un plan operativo que incluya responsables, estrategias/actividades para implementar la recomendación y fecha de cumplimento, priorizando las oportunidades de mejora de mayor criticidad de acuerdo a las necesidades del negocio.

3. Realizar una auditoría de seguimiento para verificar la adecuada implementación de las recomendaciones realizadas.

Todo esto a fin de conseguir el mejoramiento continuo de la organización y por consiguiente la eficiente y efectiva entrega de servicios de TI optimizando el servicio tanto al cliente interno como externo, satisfaciendo las necesidades y soportando los objetivos del negocio.

ANEXOS

LISTA DE VERIFICACIÓN
CONTROLES ISO 27002:2005

		SI	NO	N/A	OBSERVACIONES
1. POLÍTICA DE SEGURIDAD					
1	¿Existen políticas de seguridad aprobadas por alta gerencia y comunicadas a todo el personal?				
2	¿Existe un plan de trabajo aprobado del área de seguridad?				
	La política de seguridad es conocida por todo el personal?				
3	¿Las políticas de seguridad son revisadas periódicamente a intervalos planeados o si existen cambios significativos?				
2. ASPECTOS ORGANIZATIVOS					
3	¿Están definidas las responsabilidades de la seguridad de la información?				
4	¿Existe personal asignado a coordinar las actividades de seguridad o un comité de seguridad?				
5	¿Existen autorizaciones gerenciales para los nuevos medios de procesamiento de información?				
6	¿Existe un procedimiento para la comunicación con autoridades pertinentes (bomberos, policias, etc.) por parte de un personal designado?				
7	¿Se tiene convenios con empresas o instituciones que manejen o capaciten en temas de seguridad de la información?				
8	¿El enfoque para manejar la seguridad de la información se revisa independientemente a intervalos planeados, o cuando ocurren cambios significativos para la implementación de la seguridad?				

		SI	NO	N/A	OBSERVACIONES
9	¿Existen procedimientos y controles de seguridad para la evaluación, selección y adquisicion de hardware?				
10	¿Existen políticas para aprobación de proveedores externos?				
11	¿Se tiene procedimientos para el manejo de contratos con los proveedores externos? Ej. Contratos de mantenimientos de Hardware y Software.				
3. GESTIÓN DE ACTIVOS					
12	¿Se tiene un inventario de activos claramente identificado?				
13	¿Se tiene asignado un responsable o propietario de los activos que tiene la empresa identificado?				
14	¿Se sabe quienes son los usuarios de los activos identificados?				
15	¿Existe un criterio para valorar o clasificar los activos críticos de la organización inventariados?				
16	¿Se distingue ese criterio entre: Riesgos para el negocio, riesgos para el servicio prestado a los clientes y riesgos de continuidad de la gestion de la compañía?				
17	¿Se tiene políticas o procedimientos para el uso adecuado de los activos asignados a los empleados?				
18	¿Se han realizado pruebas de seguridad de los activos acorde al ranking que se tiene de los elementos mas críticos?				
19	¿Se tiene políticas para la clasificación de la información en base a valor, requisitos legales, sensibilidad y criticidad para la Organización?				

		SI	NO	N/A	OBSERVACIONES
20	¿Se tiene procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización?				
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS					
21	¿Se tienen definidos roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la empresa?				
22	¿Se llevan a cabo chequeos de verificación de antecedentes de los empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante?				
23	¿ Los empleados, contratistas y terceros firman acuerdos de confiencialidad o no revelacion juntos a los términos y condiciones del contrato de empleo en la empresa?				
24	¿Se identifican y revisan regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información?				
25	¿Los empleados de la organización, contratistas y terceros reciben el apropiado conocimiento, capacitación y actualización regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral?				
26	¿Existe un proceso disciplinario formal para los empleados que cometan una violación en la seguridad?				

		SI	NO	N/A	OBSERVACIONES
27	¿Existe un procedimiento a seguir para el personal reasignado o que finalice su contrato?				
28	¿Los derechos de acceso de todos los empleados a la información y medios de procesamiento de la información son eliminados a la terminación de su empleo o cambios al igual que personal de terceros?				
5. SEGURIDAD FÍSICA Y DEL ENTORNO					
29	¿Se utilizan perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información?				
30	¿Se protegen áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permite el acceso al personal autorizado?				
31	¿Se diseña y aplica seguridad física en las oficinas, habitaciones y medios?				
32	¿Se diseña y aplica protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o crado por el hombre?				
33	¿Se diseña y aplica protección física y lineamientos para trabajar en áreas seguras?				
34	¿Se aislan los medios de procesamiento de información para evitar un acceso no autorizado?				
35	¿El equipo está ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado?				

		SI	NO	N/A	OBSERVACIONES
36	¿El equipo es protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos?				
37	¿Hay políticas y procedimientos relativos al uso y protección de los equipos de la organización?				
38	¿El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información son protegidos de la intercepción o daño?				
39	¿Existe mecanismo de seguridad física en la sala de servidores?				
40	de los equipos para permitir su continua disponibilidad e integridad?				
41	¿Existe procedimientos para el manejo de la seguridad de los equipos que se encuentren fuera de la organización?				
42	¿Se asegura que se haya removido toda información confidencial y software con licencia antes de su eliminación o reutilización de un equipo?				
43	¿Existe una política de reemplazo de equipos en la empresa, donde se contemple la autorización y justificación del reemplazo, impacto de la implantación a nivel de aplicaciones y costos?				
44	¿Existen procediminentos y niveles de autorización para poder trasladar un equipo o medio de almacenamiento a otro lugar fuera de la organización?				
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES					
45	¿Los procedimientos de operación están documentados y disponibles para los usuarios que los requieran?				

		SI	NO	N/A	OBSERVACIONES
46	¿Existe un procedimiento de Control de Cambios (versiones) en los sistemas de procesamiento de información?				
47	¿Existe segregación de funciones (niveles de autorización) para modificaciones del sistema o uso de activos?				
48	¿Están separados los entornos de desarrollo, prueba y operacionales para reducir los riesgos de accesos no autorizados?				
49	¿Existe una persona responsable del paso del sistema de desarrollo a producción?				
50	¿Se realizan informes de la capacidad de uso de los recursos del sistema?				
51	¿Existen criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas?				
52	¿Se llevan a cabo las pruebas adecuadas durante su desarrollo y antes de su aceptación?				
53	¿Existe un registro de aceptación de los cambios realizados por parte de los usuarios?				
54	¿Existen controles de detección, prevención y recuperación para protegerse de código malicioso (antivirus)?				
55	¿Existe control o pistas de auditoría para el monitoreo de los servicios a terceros?				
56	¿Existe un procedimiento par la gestión de cambios de los servicios que se tiene en la organización por parte de terceros?				

		SI	NO	N/A	OBSERVACIONES
57	¿Existe un control para la detección, prevención y recuperación para software malicioso (antivirus) en la organización?				
58	¿Existen políticas de actualización de antivirus, activación periódica en las versiones instaladas en los computadores de los usuarios?				
59	¿Se realiza cursos de concienciación al personal por el uso de los equipos y sobre software malicioso?				
60	¿Se tiene procedimientos para la utilización de código móvil de acuerdo a la política de seguridad definida?				
61	Existe niveles de autorización para la ejecución de los códigos moviles dentro de la organización?				
62	¿Se realizan copias back-up o respaldo de la información y software esencial ?				
63	¿Existen procedimientos formales de verificación física de los respaldos?				
64	¿Se tiene una política para la recuperación del sistema que esté acorde a las políticas de seguridad de la empresa?				
65	¿Se administra adecuadamente la red para protegerla de amenazas y mantener la seguridad de los sistemas y aplicaciones?				
66	¿Existen procedimientos para la gestión de medios removibles?				
67	¿Existen procedimientos formales para la eliminación de medios removibles de manera segura?				
68	¿Existen procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso?				

		SI	NO	N/A	OBSERVACIONES
69	¿Existe un adecuado manejo de la seguridad para mensajería electrónica?				
70	¿Se administra el comercio electrónico de la empresa acorde a los requisitos legales?				
71	¿Se tiene un manejo de las herramientas adecuado para el comercio electrónico acorde a los contratos con terceros?				
72	¿Se tiene una política para el manejo de las transacciones en línea para prevenir el enrutamiento, alteración o divulgación no autorizada del mensaje?				
73	¿Existen pistas de auditoría y se mantienen por un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso?				
74	¿Se tiene una bitácora de actividades realizada por los operadores del sistema y administradores?				
75	¿Se tiene un registro de fallos y se toman las acciones apropiadas?				
76	¿Los relojes de los sistemas de procesamiento de información relevantes de la organización están sincronizados con una fuente de tiempo exacta acordada?				
7. CONTROL DE ACCESOS					
77	¿Existe una política de control de acceso (política de autorización) ?				
78	¿Existe un administrador que controle a los usuarios y gestione los perfiles?				
79	¿Existe un administrador que gestione las instancias de las base de datos?				
80	¿Existe un proceso de gestión formal para la asignación de claves?				

		SI	NO	N/A	OBSERVACIONES
81	¿La gerencia revisa regularmente los derechos de acceso de los usuarios utilizando un proceso formal?				
82	¿Se aplica una política de encripción de claves?				
83	¿Se tienen desahabilitados los usuarios genéricos en las aplicaciones o repositorio? Si se encuentran habilitadas estas son reseteadas de sus contraseñas genéricas.				
84	¿Se obliga cada cierto tiempo a cambiar la contraseña automáticamente?				
85	¿Se tiene políticas para la selección y uso de contraseñas?				
86	¿Existen listados de intentos de acceso no satisfactorios o denegados al repositorio o aplicaciones?				
87	¿Se les solicita a los usuarios que se aseguren de dar la protección apropiada al equipo desatendido?				
88	¿Se adopta una política de escritorio limpio para los documentos y medios de almacenamiento removibles y una política de pantalla limpia para los medios de procesamiento de información?				
89	¿Todos los usuarios tienen un id de usuario para su uso personal y exclusivo y existe una técnica de autenticación adecuada?				
90	¿Existen pistas de auditoria habilitadas para el monitorio de control de acceso a super usuarios?				
91	¿Se tiene métodos de autenticación adecuados para los accesos remotos del personal de la organización?				

		SI	NO	N/A	OBSERVACIONES
92	¿Se tiene un único registro de identificación y autenticación de usuarios para el acceso al sistema operativo?				
93	¿Se restringe y controla el uso de programas utilitarios que podrían superar al sistema y los controles de aplicación?				
94	¿Las sesiones inactivas se cierran después de un período de inactividad definido?				
95	¿Se utilizan restricciones sobre los tiempos de conexión en especial para aplicaciones de alto riesgo?				
96	¿Los sistemas sensibles tienen un ambiente de cómputo dedicado (aislado)?				
97	¿Existe una política formal de las medidas de seguridad para los recursos móviles y telecomunicaciones?				
98	¿Existen procedimientos para actividades de teletrabajo?				
8. GESTIÓN DE INCIDENTES EN LA SEG. DE LA INFORMACIÓN					
99	¿Se tiene un procedimiento para la gestión de incidentes y se toman las acciones apropiadas?				
100	¿El personal informa si ha observado alguna debilidad o sospecha de debilidad o violación de las seguridades de los sistemas?				
101	¿Existe un encargado de los procedimientos de gestión para el control de manera rápida y efectiva de los incidentes reportados?				
102	¿Existe un mecanismo para monitorear y cuantificar los incidentes reportados ?				
103	¿Se tiene un procedimiento para el manejo de las evidencias obtenidas del incidente reportado?				
104	¿Se tiene reporte de los estados de los incidentes atendidos?				

		SI	NO	N/A	OBSERVACIONES
9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
105	¿Se tiene un plan de continuidad del negocio o contingencia acorde a los objetivos de la organización?				
106	¿El plan de continuidad de negocio es revisado periódicamente por la alta gerencia?				
107	¿El plan se encuentra difundido formalmente en la organización?				
108	¿Existe un responsable de la seguridad en caso de contingencia?				
109	¿En el plan se identifican todos los riesgos, probabilidad de ocurrencia de impacto y sus posibles alternativas de solución?				
110	¿Están definidos formalmente los procedimientos manuales de los procesos claves que se pondrían en ejecución en caso de una contingencia?				
111	¿Se han realizado pruebas de eficacia al plan de continuidad de negocio?				
112	¿Existe un procedimiento que garantice la continuidad y disponibilidad del equipo de cómputo en caso de desastre o contingencia?				

BIBLIOGRAFÍA

1. Estándar Internacional ISO/IEC 27001.
2. Estándar Internacional ISO/IEC 27002:2005.
3. Resolución JB-2005-834 de la Superintendencia de Bancos y Seguros – Sección 2, Artículo 4.
4. Material de los módulos "Seguridad de la Información y Seguridad Informática" y "Planificación de Contingencias para la recuperación de Desastres" – V Diplomado Superior en Auditoría Informática – ESPOL.
5. Páginas Web de información especializada:
   - http://www.iso27000.es
   - http://www.iso27001certificates.com