Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo Final de Máster

Plan Director de Seguridad de la Información

Alexander Larrahondo Nuñez

2013

Contenido

Índice de Tablas

1. PLAN DIRECTOR DE SEGURIDAD

Fase 1: Contextualización y Documentación

1.1 Introducción

A continuación se realizara una introducción a las normas ISO 27001 e ISO27002 que usaremos como base para el desarrollo de este trabajo, la norma ISO 27001 es un estándar para la seguridad de la información (Information Technology – Security Techniques – Information Security System – Requirements) fue aprobado como estándar internacional en 2005 por la ISO (International Organization for Standardization), en este estándar se especifican los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de seguridad de la información, basado en el ciclo de Deming PDCA (Plan, Do, Check, Act), la norma ISO 27002 es el estándar para la seguridad de la información publicado anteriormente como ISO/IEC 17999:2000 por la ISO, con origen en el British Standard BS 7799-1, la norma ISO 27001 es certificable, mientras que en la norma 27002 es en general un conjunto de buenas prácticas y controles sugeridos que se deben revisar si aplican o no dependiendo de cada caso en particular

1.2 Descripción de la Organización de Estudio

La empresa seleccionada para la elaboración del trabajo final del Master que consiste en la elaboración de un “Plan de Seguridad de la Información” basados en la implementación y cumplimiento de la normativa ISO/IEC 27001: 2005 y en los controles de la normativa ISO/IEC 27002, es una empresa ubicada en Bogotá Colombia perteneciente al sector financiero dedicada a la administración y desarrollo de sistemas de pago de bajo valor, estructuradora y gestora de negocios para el sector financiero, vigilada por la Superintendencia Financiera (Entidad gubernamental encargada de supervisar los sistemas financiero y bursátil del mercado colombiano, a partir del decreto 1400 del 2005)

1.3 Actividad y Entorno

La compañía cuenta al día de hoy con más de 40 años de existencia, la compañía al manejar datos de tarjetahabientes es sujeta al cumplimiento de normativas de seguridad locales (circular externa 042 Superintendencia Financiera de Colombia, etc) e internacionales, específicamente el estándar PCI-DSS (Payment Card Industry Data Security Standard).

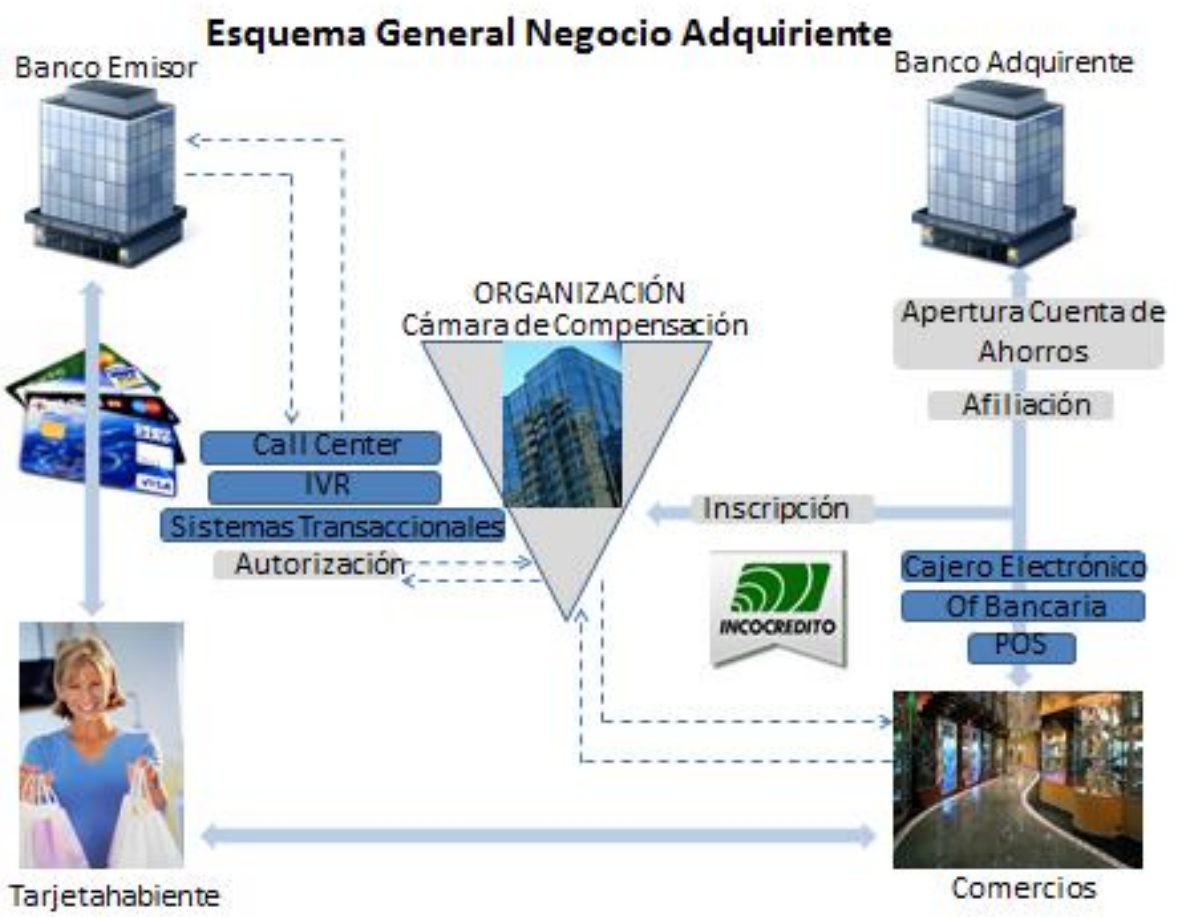
El sector financiero a nivel mundial es el que cuenta con las más fuertes y estrictas normativas en cuanto al manejo de la información de los clientes, y en especial las compañías del sector financiero que procesan, almacenan y/o transmiten datos de tarjetahabientes normativas impulsadas por los comités conformados por las grandes marcas de tarjetas de crédito a nivel mundial, que autorizan a los procesadores de pago de bajo valor a usar sus nombres por medio de franquicias basadas en el cumplimiento de ciertas normas, entre las que se incluyen certificaciones formales en normativa PCI-DSS que son evaluadas a través de auditores autorizados QSA's (Qualified Security Assessor), la norma tiene 6 objetivos de control, con un total de 12 requisitos en cada uno de los cuales hay definidos uno o más controles.

La normas PCI-DSS (Payment Card Industry Data Standard) o estándar de seguridad de datos para la industria de tarjetas de pago, es el estándar desarrollado por el PCI SSC (Payment Card Industry Security Standards Council) pensado como una guía que ayuda a las entidades que procesan, almacenan y/o transmites datos de tarjetahabientes con el fin de asegurar esta información y prevenir los fraudes que se puedan presentar con el uso indebido de esta información, dado que estas normas tienen como finalidad la protección de los datos de tarjetahabientes como su principal objetivo, los sistemas de información que no tienen datos de tarjetahabientes no son objetivo de esta norma, en una revisión de alguno de los auditores autorizados o QSA's se hace énfasis en el CDE O Cardholder Data Enviroment por lo que los demás sistemas de apoyo que necesitan ser protegidos no están dentro del alcance, en este sentido el estándar PCI DSS no tendrá el mismo alcance desde el punto de vista de activos de información que el conjunto de normas ISO 27001 e ISO 27002 que son las que nos ocupan

El decreto 1400 de 2005 establece que son de bajo valor "aquellos sistemas de pago que procesan órdenes de transferencia o recaudo, incluyendo aquellas derivadas de la

utilización de tarjetas de crédito o débito, por un valor promedio diario que sea inferior a “2.5 billones, monto que se ajusta anualmente de acuerdo con el IPC (Índice de precios al consumidor) del DANE (Departamento Nacional de Estadística)

A continuación veremos en un diagrama el esquema general del negocio adquirente con sus diferentes actores



Grafica 1. Diagrama General negocio

Para la gráfica uno en el negocio de adquirencia, la organización hace el papel de cámara de compensación entre los diferentes actores del negocio de pago de bajo valor, puntualmente en este esquema la organización se encarga a través de varios sistemas (call center, IVR, y diferentes sistemas transaccionales) de compensar entre el banco emisor y el banco adquirente las transacciones que los tarjetahabientes han realizado a través de su red de POS (Point Of Sales, puntos de venta) o datafonos ubicados en los comercios, o también los retiros en cajeros o en oficinas bancarias aliadas

1.4 Tamaño y Estructura Organizacional

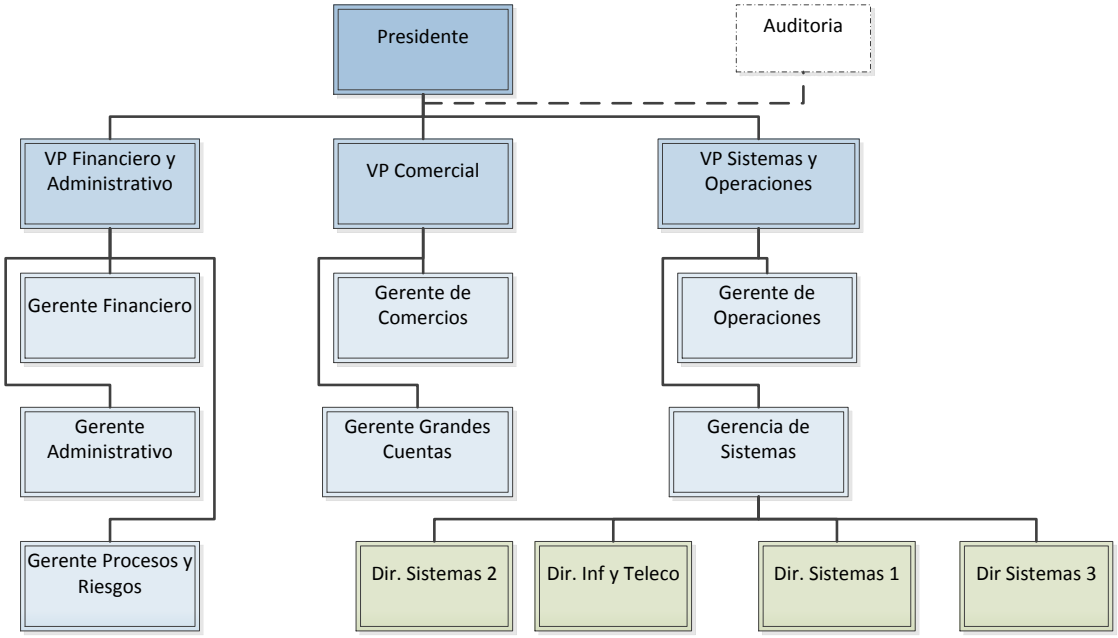
La organización tiene oficinas en 17 ciudades del país, y cuenta con una nómina de 720 empleados, la compañía cuanta con varias vicepresidencias entre las que están la vicepresidencia de sistemas y operaciones, la vicepresidencia comercial, y la vicepresidencia financiera y administrativa y la vicepresidencia de sistemas y operaciones, de ellos cerca de 100 empleados son del área de tecnología, divididos en varias direcciones entre las que están diseño y desarrollo e infraestructura, además de las otras áreas normales en una organización como son financiera y contable, administrativa, compras, recursos humanos, servicios generales y el área comercial, en el área de infraestructura y telecomunicaciones se administran todos los elementos de infraestructura de la organización y todos los equipos de telecomunicaciones y de seguridad por lo que es una de las direcciones más relevantes desde el punto de vista del negocio se encuentran los operadores del centro de cómputo que está atendiendo los procesos que se ejecutan en los sistemas durante las 24 horas del día y grupo de ingenieros atendiendo en turnos rotativos el monitoreo de los diferentes canales de comunicaciones con los comercios y con los bancos, se cuenta además con un esquema de mesa de ayuda que presta soporte en temas de informática (Portatiles, PC's, software de ofimática y software propio de la organización) y que atienden las solicitudes en horario laboral.

En el área de Telecomunicaciones e infraestructura para las incidencias fuera de horario los operadores del centro de cómputo, contactan al teléfono móvil de los ingenieros que administran las diferentes plataformas y que cuentas con accesos remotos a través de VPN's client to site con doble factor de autenticación, para poder atender de manera oportuna los incidentes que se presenten, si el incidente requiere la presencia del ingeniero, este deberá desplazarse hasta la compañía.

Existen tres direcciones de sistemas adicionales, una en donde se atienden las solicitudes de diseño y desarrollo de los aplicativos especializados de la organización y en donde se atienden también los proyectos que en razón de sus necesidades en tiempo o en recursos no se pueden atender con los recursos propios y que se contratan con empresas externas, en otra de las direcciones se hace la administración del switch transaccional y los procesos que en se ejecutan y en los cuales se incluyen la interacción los demás

sistemas de la organización y con los socios de negocios, en otra de las direcciones se atienden los procesos y proyectos que tienen que ver con los medios de acceso (Datafonos en POS)

La responsabilidad sobre los temas de seguridad, recae en todas las áreas de la compañía, pero en especial en el área de tecnología quien administra las herramientas de seguridad informática con que se cuenta con el fin de cumplir con los diferentes requerimientos, y el área de riesgos, en donde se definen y establecen las políticas de seguridad a cumplir.



Grafica 2: Organigrama Organizacional

1.5 Definición de Objetivos del Plan Director de Seguridad

El plan director de seguridad como hoja de ruta que debe seguir la compañía para conseguir gestionar de forma adecuada la seguridad tendrá como alcance los sistemas transaccionales de la organización en donde se hace almacenamiento, transmisión, modificación o uso de datos de tarjetahabientes, para la definición del plan director de seguridad se deberán contemplar los siguientes objetivos:

1. Garantizar la confidencialidad, integridad y disponibilidad de la información de los tarjetahabientes en los sistemas de información de la organización que capturen, transmitan, almacenen y/o procesos dicha información.
2. Establecer de manera claro los requisitos de seguridad de la información que la compañía debe cumplir con el fin de garantizar la protección de la información de las diferentes amenazas a las que está expuesta, minimizando los riesgos, con el fin de cumplir con sus obligaciones para con los clientes, accionistas y colaboradores, garantizando con ello la continuidad del negocio
3. Realizar un análisis diferencial del estado actual del estado de seguridad de los activos de la compañía, versus el cumplimiento de la norma ISO/IEC 27001 e ISO/IEC 27002, para que a partir de este análisis se identifiquen los recursos necesarios y se puedan establecer los planes de trabajo con el fin de cumplir las normas.

1.6 Sistemas de Información que dan soporte a la Organización

Al igual que muchas otras organizaciones la búsqueda de la automatización de los procesos ha genero la utilización de múltiples sistemas al interior, para hacer claridad acerca de los sistemas de información que van a ser objeto de este Plan Director de Seguridad Informática, los describiremos de manera general en este apartado, relacionándolos con las funciones que desempeñan dentro de la estructura general del negocio.

Los sistemas de POS que se usan en los comercios están conectados a través de canales privados de comunicaciones, la información de las transacciones llega a la red corporativa y de allí se enrutan al switch transaccional, que es un sistema HP Non-Stop en donde se realiza la autorización de las transacciones, las autorizaciones se evalúan solicitando a los sistemas centrales de los diferentes bancos emisores de las tarjetas la autorización o negación de la misma en tiempo real, las transacciones autorizadas o denegadas quedan almacenadas en el sistema y en horas de la madrugada el sistema de canje y compensación que es un sistema basado en OS 400 realiza los procesos de canje y compensación de nuevo basado en comunicaciones en tiempo real contra los sistemas de los bancos, este sistema determina los valores a cobrar por las diferentes

transacciones autorizadas o negadas por cada banco y el cruce de cuentas entre los saldos positivos y negativos entre los bancos para determinar si tienen saldos a favor o en contra y contra cuál de los demás bancos deberán realizar los pagos respectivos, para la información que no es en línea con los bancos o con algunos en donde los límites de autorizaciones se manejan en la organización o para cuando por fallas en los canales de comunicación no se puede autorizar directo contra los sistemas de los bancos y de acuerdo a lo que se haya negociado con ellos para estos casos se usan varios procesos apoyados en el intercambio seguro de información con los diferentes actores del proceso a través del sistema de intercambio de archivos de la organización, que es un sistema Windows que usa un software llamado EFT Server.

Existe además un sistema de comercio electrónico que le permite a los comercios a través de web services y de VPN's conectar con el sistema de la organización y autorizar compras de manera presencial y no presencial (realizando a su vez las validaciones necesarias de los datos de los tarjetahabientes contra los bancos respectivos), este sistema es un sistema basado en Sistema Operativo AIX con soporte de base de datos Oracle, a nivel de sistemas transaccionales estos son los más significativos, cada uno de estos sistemas cuenta con sus amientes de pruebas y de contingencia y para sistemas de apoyo adicionales en las labores administrativas de la organización se cuenta con sistemas de ERP, un sistema de Nomina, una red de Windows con un sistema de correo electrónico basado en Lotus Notes y los dispositivos de seguridad perimetral y de comunicaciones necesarios para hacer que todos estos sistemas funcionen de manera adecuada y den servicios a los usuarios internos y externos que los requieran.

Podemos resumir que el alcance del Plan Director de Seguridad de la Información serán los activos de la información que dan soporte a los sistemas transaccionales críticos de la organización en donde se almacenan, transmiten o manipulan datos de tarjetahabientes

1.7 Análisis diferencial del estado actual versus ISO/IEC 27001 y 27002

Dada la naturaleza del negocio, en donde se gestionan y transmiten datos de tarjetahabientes, la compañía está 5 certificada en el estándar PCI-DSS, y su nivel de

madurez es alto, en esta normativa cuyo énfasis en proteger los datos de los tarjetahabientes en su transmisión, modificación y/o almacenamiento.

A continuación se anexa una tabla con la lista de controles de ISO 27002:2009 en donde se relacionan el nivel de cumplimiento con el control estimado en un porcentaje y unas observaciones sobre el porcentaje faltante

				% Cumplimiento	Observaciones
5	POLITICA DE SEGURIDAD				
	5.1	Politica de Seguridad de la Información			
		5.1.1	Documento de Politica de Seguridad de la Información	100%	
		5.1.2	Revisión de la Politica de Seguridad de la Información	100%	
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN				
	6.1	Organización Interna			
		6.1.1	Compromiso de la dirección con la seguridad de la Información	100%	
		6.1.2	Coordinación de la Seguridad de la Información	100%	
		6.1.3	Asignación de responsabilidades realtivas a la Seguridad de la Información	100%	
		6.1.4	Proceso de Autorización de recursos para el tratamiento de la Información	100%	
		6.1.5	Acuerdos de Confidencialidad	90%	Faltan Algunos contratos con Terceros
		6.1.6	Contacto con las autoridades	90%	Falta sistematizar y centralizar la Información
		6.1.7	Contacto con grupos de especial Interes	90%	Falta sistematizar y centralizar la Información
		6.1.8	Revisión independiente de la seguridad de la información	100%	
	6.2	Terceros			
		6.2.1	Identificación de los riesgos derivados del acceso de terceros	90%	Terminar de documentar y formalizar
		6.2.2	Tratamiento de la seguridad en la relación con los clientes	90%	Terminar de documentar y formalizar
		6.2.3	Tratamiento de la seguridad en contratos con terceros	90%	Faltan por revisar algunos contratos
7	GESTION DE ACTIVOS				
	7.1	Responsabilidad sobre los activos			
		7.1.1	Inventario de Activos	75%	Falta centralizar y consolidar la información
		7.1.2	Propiedad de los Activos	100%	
		7.1.3	Uso aceptable de los activos	80%	Falta documentar
	7.2	Clasificación de la Información			
		7.2.1	Directrices de clasificación	100%	
		7.2.2	Etiquetado y Manipulado de la Información	90%	Falta revisar que las áreas esten cumpliendo
8	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS				
	8.1	Antes del empleo			
		8.1.1	Funciones y Responsabilidades	85%	Debido al crecimiento falta documentar
		8.1.2	Investigación de Antecedentes	100%	
		8.1.3	Terminos y Condiciones de Contratación	100%	
	8.2	Durante el empleo			
		8.2.1	Responsabilidades de la Dirección	85%	Falta Documentar
		8.2.2	Concientización, formación y capacitación en Seguridad de la Información	100%	
		8.2.3	Proceso Disciplinario	85%	Falta Documentar
	8.3	Cese del Empleo o cambio de Puesto de Trabajo			
		8.3.1	Responsabilidad del Cese o Cambio	75%	Terminar de documentar y formalizar
		8.3.2	Devolución de Activos	30%	Terminar de documentar y formalizar
		8.3.3	Retirada de los derechos de Acceso	95%	Falta verificar
9	SEGURIDAD FISICA Y DEL ENTORNO				
	9.1	Areas Seguras			
		9.1.1	Perimetro de Seguridad Fisica	100%	
		9.1.2	Controles Fisicos de Entrada	100%	
		9.1.3	Seguridad de Oficinas, despachos e instalaciones	100%	
		9.1.4	Protección contras las amenazas externas y de origen ambiental	90%	Terminar de documentar y formalizar
		9.1.5	Trabajo en áreas seguras	90%	Terminar de documentar y formalizar
		9.1.6	Areas de acceso cliente y de carga y descarga	??	
	9.2	Seguridad en los equipos			
		9.2.1	Ubicación y protección de equipos	80%	Terminar de documentar y formalizar
		9.2.2	Servicios de suministro	90%	Terminar de documentar y formalizar
		9.2.3	Seguridad del Cableado	90%	Terminar de documentar y formalizar
		9.2.4	Mantenimiento de los equipos	85%	Formalizar los registros
		9.2.5	Seguridad de los equipos fuera de las instalaciones	85%	Documentar y formalizar un procedimiento
		9.2.6	Seguridad en la reutilización o eliminación de los equipos	95%	Documentar y formalizar dentro de un Proced
		9.2.7	Retirada de activos	95%	Documentar y formalizar dentro de un Proced

10	GESTION DE COMUNICACIONES Y OPERACIONES				
	10.1	Responsabilidad y procedimientos de Operación			
		10.1.1	Documentación de los procedimientos de Operación	80%	Faltan documentar algunos proc de Operación
		10.1.2	Gestion de cambios	90%	Faltan documentar los proc de Emergencia
		10.1.3	Segregación de funciones	95%	Documentar la Segregación de funciones
		10.1.4	Separación de recursos de desarrollo, prueba y operación	75%	Falta segregación en algunos de los ambientes
	10.2	Gestion de la Prestación del servicio por terceros			
		10.2.1	Prestación del Servicio	90%	Oficializar controles con terceros
		10.2.2	Monitoreo y revisión de los servicios prestados por terceros	90%	Documentar y formalizar dentro de un Proced
		10.2.3	Gestion del cambio en los servicios prestados por terceros	85%	Documentar y formalizar dentro de un Proced
	10.3	Planificación y aceptación del sistema			
		10.3.1	Gestion de la capacidad	85%	Terminar de documentar y formalizar
		10.3.2	Aceptación del Sistema	25%	No existen los controles de aceptación del Sistema
	10.4	Protección contra el codigo malicioso y descargable			
		10.4.1	Controles contra el codigo malicioso	100%	Procedimientos maduros
		10.4.2	Controles contra el codigo descargado en el cliente	100%	Procedimientos maduros
	10.5	Copias de Seguridad			
		10.5.1	Copias de seguridad de la información	85%	Faltan documentar algunos proc de Operación
	10.6	Gestion de la Seguridad de las Redes			
		10.6.1	Controles de Red	95%	Falta actualizar alguna Documentación
		10.6.2	Seguridad de los Servicios de Red	95%	Falta actualizar algunos de los documentos
	10.7	Manipulación de los Soportes			
		10.7.1	Gestion de Soportes Extraibles	95%	Procedimientos Maduros
		10.7.2	Retirada de soportes	85%	Documentar y formalizar dentro de un Proced
		10.7.3	Procedimiento para el manejo de la información	85%	Documentar y formalizar dentro de un Proced
		10.7.4	Seguridad de la Documentación del Sistema	85%	Documentar y formalizar dentro de un Proced
	10.8	Intercambio de Información			
		10.8.1	Politicas y procedimientos de Intercambio de Información	85%	Documentar y formalizar dentro de un Proced
		10.8.2	Acuerdos de Intercambio	85%	Documentar y formalizar dentro de un Proced
		10.8.3	Soportes fisicos en transito	85%	Documentar y formalizar dentro de un Proced
		10.8.4	Mensajeria electronica	85%	Documentar y formalizar dentro de un Proced
		10.8.5	Sistemas de información empresariales	85%	Documentar y formalizar dentro de un Proced
	10.9	Servicios de comercio electrónico			
		10.9.1	Comercio Electrónico	80%	Documentar y formalizar dentro de un Proced
		10.9.2	Transacciones en Linea	90%	Documentar y formalizar dentro de un Proced
		10.9.3	Información Publicamente Disponible	90%	Documentar y formalizar dentro de un Proced
	10.1	Monitoreo			
		10.10.1	Registros de Auditoria	90%	Documentar y formalizar dentro de un Proced
		10.10.2	Monitoreo del uso del sistema	80%	Revisar Alcance del Monitoreo
		10.10.3	Protección de la información de los registros	70%	Falta centralizar la información y documentar
		10.10.4	Registros de administración y operación	70%	Falta controlar las actividades de los administradores
		10.10.5	Registro de Fallos	90%	Documentar y formalizar dentro de un Proced
		10.10.6	Sincronización del Reloj	90%	Documentar y formalizar dentro de un Proced
11	CONTROL DE ACCESO				
	11.1	Requisitos de negocio para el control de acceso			
		11.1.1	Politica de control de acceso	90%	Documentar y formalizar dentro de un proced
	11.2	Gestion de acceso de usuario			
		11.2.1	Registro de Usuarios	95%	Revisar que el procedimiento ese actualizado
		11.2.2	Gestion de Privilegios	85%	Documentar y formalizar dentro de un proced
		11.2.3	Gestion de Contraseñas de Usuario	95%	Revisar que el procedimiento ese actualizado
		11.2.4	Revisión de los derechos de acceso de usuario	85%	Documentar y formalizar dentro de un Proced
	11.3	Responsabilidades de Usuario			
		11.3.1	Uso de contraseñas	85%	Revisar que el procedimiento ese actualizado
		11.3.2	Equipo de usuario desantendido	95%	Revisar que el procedimiento ese actualizado
		11.3.3	Politica de puesto de trabajo Despejado y pantalla limpia	95%	Revisar que el procedimiento ese actualizado
	11.4	Control de Acceso a la red			
		11.4.1	Politica de uso de los servicios en red	95%	Documentar y formalizar dentro de un Proced
		11.4.2	Autenticación de usuario para conexiones externas	90%	Documentar y formalizar dentro de un Proced
		11.4.3	Identificación de los equipos en las redes	40%	Documentar y formalizar dentro de un Proced
		11.4.4	Protección de los puertos de diagnostico y configuración remotos	80%	Documentar y formalizar dentro de un Proced
		11.4.5	Segregación de las redes	95%	Revisar que el procedimiento ese actualizado
		11.4.6	Control de la conexión a la red	95%	Revisar que el procedimiento ese actualizado
		11.4.7	Control de encaminamiento (routing) de red	95%	Documentar y formalizar dentro de un Proced
	11.5	Control de acceso al sistema Operativo			
		11.5.1	Procedimientos seguros de inicio de sesión	75%	Documentar y formalizar dentro de un Proced
		11.5.2	Identificación y autenticación de usuario	95%	Revisar que el procedimiento ese actualizado
		11.5.3	Sistema de gestion de contraseñas	90%	Faltan unicar algunos de los sistemas propietarios
		11.5.4	Uso de los recursos del sistema	90%	Revisar que el procedimiento ese actualizado
		11.5.5	Desconexión automática de sesión	85%	Algunos de los sistemas no tienen esta caracteristica
		11.5.6	Limitación del tiempo de conexión	85%	Verificar esta caracteristica en elgunos sistemas
	11.6	Control de acceso a las aplicaciones y a la Información			
		11.6.1	Restricción del acceso a la información	95%	Revisar que el procedimiento ese actualizado
		11.6.2	Aislamiento de sistemas sensibles	95%	Revisar que el procedimiento ese actualizado
	11.7	Ordenadores portátiles y teletrabajo			
		11.7.1	Ordenadores portátiles y comunicaciones móviles	75%	Faltan politicas para dispositivos moviles
		11.7.2	Teletrabajo	40%	No hay politica oficial de Teletrabajo

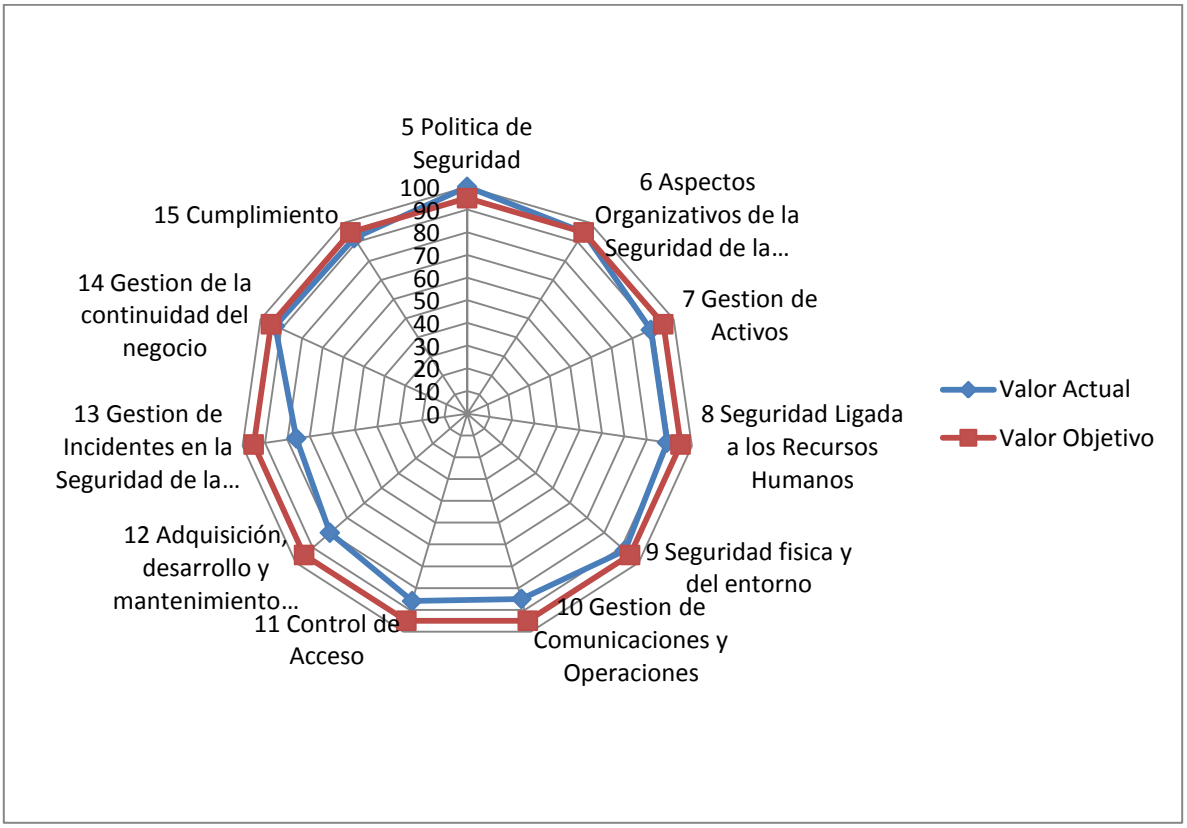
12	ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN				
	12.1	Requisitos de Seguridad de los sistemas de información			
		12.1.1	Analisis y especificación de los requisitos de Seguridad	40%	Falta documentar y oficializar el control
	12.2	Tratamiento correcto de las aplicaciones			
		12.2.1	Validación de los datos de entrada	60%	Documentar y oficializar los controles
		12.2.2	Control de procesamiento Interno	60%	Documentar y oficializar los controles
		12.2.3	Integridad de los mensajes	70%	Documentar y oficializar los controles
		12.2.4	Validación de los datos de salida	90%	Documentar y oficializar los controles
	12.3	Controles Criptograficos			
		12.3.1	Politica sobre el uso de uso de controles criptograficos	85%	Documentar y oficializar los controles
		12.3.2	Gestion de claves	85%	Revisar qu el procedimieo
	12.4	Seguridad de los archivos de sistema			
		12.4.1	Control del software operativo	95%	Revisar que el procedimiento este actualizado
		12.4.2	Protección de los datos de pruebas del sistema	60%	Verificar la correcta segregación de ambientes
		12.4.3	Control de acceso al código fuenre de los programas	95%	Revisar que el procedimiento este actualizado
	12.5	Seguridad en los procesis de desarrollo y soporte			
		12.5.1	Procedimientos de control de cambios	95%	Revisar que el procedimiento este actualizado
		12.5.2	Revisión Técnica de las aplicaciones tras efectuar cambios en el S.O.	85%	Revisar que el control este incluido en el procedimiento
		12.5.3	Restricciones a los cambios en los paquetes de software	95%	Revisar que el control este incluido en el procedimiento
		12.5.4	Fugas de Información	90%	Revisar que el procedimiento este actualizado
		12.5.5	Desarrollo del software contratato externamente	75%	Documentar y oficializar los controles
	12.6	Gestión de la vulnerabilidad técnica			
		12.6.1	Control de las vulnerabilidades tecnicas	95%	Revisar que el procedimiento este actualizado
13	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN				
	13.1	Notificación de Eventos y puntos debiles de seguridad de la Información			
		13.1.1	Reporte sobre los eventos de seguridad de la Información	95%	Revisar que el procedimiento este actualizado
		13.1.2	Reporte sobre las debilidades en la seguridad	40%	Documentar y oficializar los controles
	13.2	Gestión de Incidentes y mejoras de seguridad de la Información			
		13.2.1	Responsabilidades y Procedimientos	95%	Revisar que el procedimiento este actualizado
		13.2.2	Aprendizaje de los incidentes de seguridad de la Información	75%	Documentar y oficializar los controles
		13.2.3	Recopilación de evidencias	75%	Documentar y oficializar los controles
14	GESTIONDE LA CONTINUIDAD DEL NEGOCIO				
	14.1	Aspectos de seguridad de la información en la gestion de la continuidad del negocio			
		14.1.1	Inclusión de la seg de la info en el proceso de gestion de la Continuidad del	95%	Revisar que el procedimiento este actualizado
		14.1.2	Continuidad del negocio y evaluación de riesgos	95%	Revisar que el procedimiento este actualizado
		14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seg de l	95%	Revisar que el procedimiento este actualizado
		14.1.4	Marco de referencia para la planificación de la continuidad del negocio	95%	Revisar que el procedimiento este actualizado
		14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad	85%	Revisar que el procedimiento este actualizado
15	CUMPLIMIENTO				
	15.1	Cumplimiento de los requisitos legales			
		15.1.1	Identificación de la lesgislación aplicable	95%	Revisar que el procedimiento este actualizado
		15.1.2	Derecho de propiedad intelectual	95%	Revisar que el procedimiento este actualizado
		15.1.3	Protección de los documentos de la organización	95%	Revisar que el procedimiento este actualizado
		15.1.4	Protección de datos y privacidad de la información de carácter personal	95%	Revisar que el procedimiento este actualizado
		15.1.5	Prevención del uso indebido de recursos de tratamiento de la Información	95%	Revisar que el procedimiento este actualizado
		15.1.6	Regulación de los controles criptográficos	95%	Revisar que el procedimiento este actualizado
	15.2	Cumplimiento de las politicas y normas de seguridad y cumplimiento técnico			
		15.2.1	Cumplimiento de las políticas y normas de seguridad	95%	Revisar que el procedimiento este actualizado
		15.2.2	Comprobación del cumplimiento técnico	60%	Documentar y oficializar los controles
	15.3	Consideraciones sobre las auditorias de los sistemas de información			
		15.3.1	Controles de auditoria de los sistemas de información	95%	Revisar que el procedimiento este actualizado
		15.3.2	Protección de las herramientas de auditoria de los sistemas de información	95%	Revisar que el procedimiento este actualizado

Tabla 1: Análisis Diferencial ISO 27001 e ISO 27002

Como resultado del análisis diferencial podemos mostrar una gráfica de dispersión en donde se observan los valores objetivos de todos los objetivos de control, establecidos por la dirección de la empresa en al menos el 95% dando margen del 5% en su cumplimiento como un valor realista del mismo.

En algunos objetivos de control tal y como se observa en la tabla hacen falta ajustes menores como verificación de la documentación y otros en donde en necesario emprender acciones para mejorar los porcentajes de cumplimiento con el fin de llegar al porcentaje de cumplimiento definido por la organización, para estos casos será necesario

establecer los planes de acción necesarios dentro de los que se definirán los recursos humanos y un estimado de los recursos económicos para poderlos llevar a cabo.



Grafica 3: Representación gráfica grado de madurez ISO 27001 e ISO 27002

Como se puede observar en la gráfica 3, en varios de los objetivos de control se han alcanzado los niveles de madurez óptimos definidos por la organización, permitiendo una evolución del sistema y de su seguridad, demostrando el progreso que permite minimizar el riesgo y el impacto de las amenazas que mitigan estos objetivos de control y en varios de los otros objetivos de control no se ha logrado el valor objetivo de madurez.

Fase 2: Sistema de Gestión Documental

2.1 Política de Seguridad de la Información

A continuación se describirá la política de seguridad de la información de la organización: Para la organización la seguridad de la información de sus clientes y de los usuarios de los sistemas que se gestionan y/o operan es de vital importancia y se protegerá de cualquier perdida en su confidencialidad, integridad y disponibilidad mediante la implementación de controles manuales o automáticos en los procesos, la tecnología y la gente asociada a su generación, tratamiento, transmisión y almacenamiento con el fin de garantizar su correcto tratamiento respetando las normales legales vigentes.

2.2 Declaración de Aplicabilidad

La política de seguridad de la información de la organización, aplica pero no se limita a:

- La información de sus clientes, socios de negocios, proveedores y clientes finales
- La información generada como resultado de las operaciones normales del negocio
- Todos los activos de información a través de su ciclo de vida, incluyendo creación, transmisión, almacenamiento y disposición final, priorizando su protección de acuerdo con las evaluaciones de riesgos
- Los diferentes ambientes de procesamiento de información que incluyen producción, pruebas, contingencia y certificación
- Todos los recursos humanos que participen del ciclo del negocio de la organización incluyendo contratistas y terceros

En el documento anexo de declaración de aplicabilidad esta la tabla con todos los controles de la norma en donde se observa si existen controles, y la razón de la selección de cada uno de ellos, resaltando si el control surge de un requerimiento legal, de una obligación contractual, de un requerimiento de negocio o de las mejores prácticas, o si el control surge como resultado del análisis de riesgos realizado a los activo de información de la organización

2.3 Documentación del SGSI

Como parte de la documentación del Sistema de Gestión de Seguridad de la Información tenemos entre otros los siguientes documentos

- Procedimientos de Auditorías Internas
- Gestión de Indicadores
- Procedimiento de Revisión por la Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos

Para cada uno de estos documentos tenemos la misma estructura con el fin de conservar una consistencia en toda la documentación, la estructura del documento contendrá además de un encabezado en donde se registrara el nombre del procedimiento, su identificador nemotécnico, la versión del procedimiento, la fecha desde la cual está vigente la versión del procedimiento, el responsable del mismo, el área a la cual pertenece el procedimiento, y la numeración de página del mismo, además tendrá los siguientes componentes

- Un cuadro de control de cambios
- Objetivo
- Alcance
- Definiciones
- Políticas
- Diagrama de actividades y controles internos
    - Diagrama de Flujo
    - Notas aclaratorias
    - Matriz de Riesgos y Controles

Para el desarrollo de la documentación del Sistema de Gestión de Seguridad de la Información desarrollaremos varios de los documentos bases y se entregaran como anexos documentales del mismo, los documentos a entregar son los siguientes:

Anexo Documental 1. Políticas de Seguridad de la Información

Anexo Documental 2. Procedimiento de Auditorías Internas

Anexo Documental 3. Procedimiento de Gestión de Indicadores

Anexo Documental 4. Procedimiento de Gestión de Roles y Responsabilidades

Anexo Documental 5. Procedimiento de Revisión por la Dirección

Fase 3: Análisis de Riesgos

3.1 Metodología

La realización del análisis de riesgos tiene como fin identificar de manera clara los riesgos a los cuales está expuesta la organización, y basados en esta identificación de los riesgos determinar cuáles medidas de seguridad serán las adecuadas para los diferentes activos de seguridad de la información, de igual manera permite establecer los planes de contingencia, para este caso realizaremos un análisis de riesgo residual, que es un tipo de análisis que se realiza teniendo en cuentas las medidas de seguridad que la organización ya tiene planteadas, como resultado de este tipo de análisis se obtiene el riesgo real al cual están expuestos los diferentes activos de la información que tiene la organización.

De las diferentes metodologías existentes en el mercado, se optó por utilizar NIST 800-30 dado que esta metodología que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías y comunicaciones (TIC's) y en consideración a que los riesgos que sean identificados quedaran expresados en valores económicos lo que facilita la toma de decisiones de parte del equipo directivo.

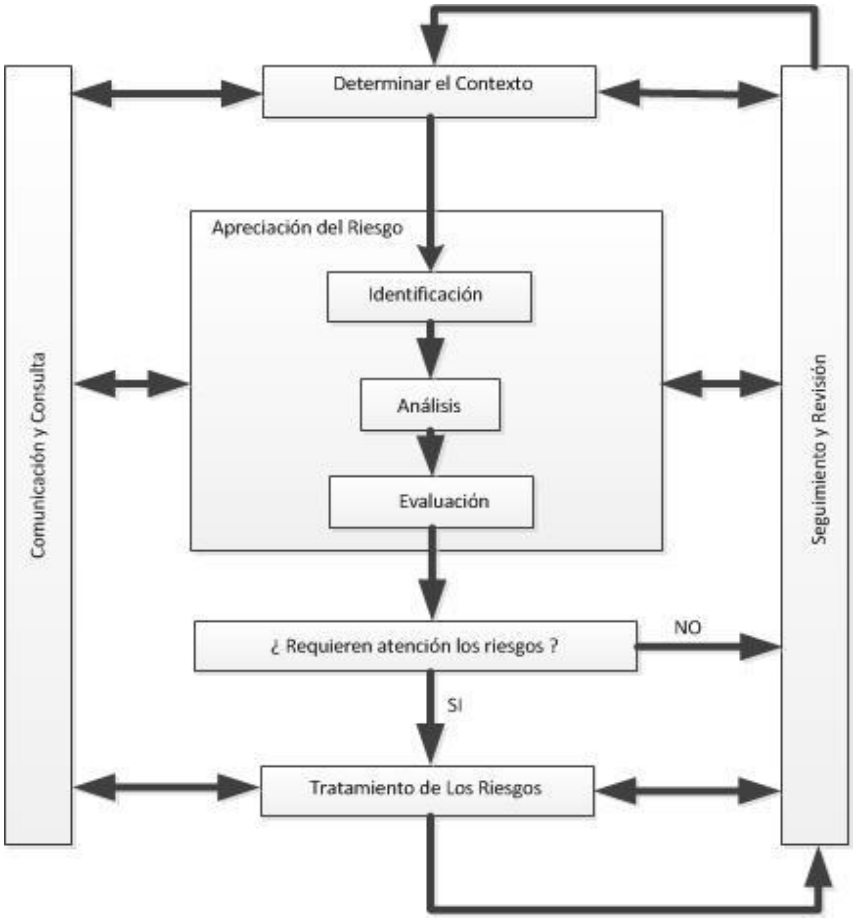
El análisis de riesgos considera los siguientes elementos

1. Activos: Son los recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objeticos propuestos por la dirección
2. Amenazas: Son las situaciones o hechos que pueden producir daño y que les pueden pasar a los activos causando un perjuicio a la organización
3. Vulnerabilidades: Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo de la información
4. Impacto: Daño causado sobre el activo de la información una vez se materializa una de las vulnerabilidades, conociendo el valor de los activos es más sencillo estimar el valor del impacto

5. Riesgo: Es la probabilidad de que una amenaza se materialice y afecte a los activos de la información
6. Salvaguardas: Mecanismo de protección frente a las amenazas

3.2 Proceso de Gestión de Riesgos

La gestión de riesgo se puede definir como un proceso de toma de decisiones en un ambiente de incertidumbre sobre una acción que puede suceder y sobre las consecuencias que existirán si dicha acción sucede, para ilustrar un poco el proceso de gestión de riesgo y cómo interactúan en el sus diferentes elementos, anexamos el diagrama siguiente:



Grafica 4: Diagrama de Proceso de Gestión de Riesgos (Tomado Magerit Versión 3)

Una vez contemplados los anteriores elementos para el análisis de riesgo, las opciones ante los riesgos son las siguientes

- Aceptarlo: Significa que la organización en cabeza del comité de riesgos y procesos decide no emprender ninguna acción, en este caso se asume el impacto en caso de que se materialice el riesgo, en tal caso si se produce un incidente se procederá a la recuperación esta opción no debería darse para riesgos altos o que comprometan activos de información relevantes para la organización, es una acción aceptable ante activos de información despreciables (desde el punto de vista de importancia para la organización, así su costo pueda ser alto)
- Mitigarlo: Esta opción es la que más se presenta luego de los análisis de riesgos respectivos, y significa que una vez la organización identifica un riesgo, se aplican salvaguardas o medidas de protección que buscan minimizar o reducir el riesgo, para que en caso de que la amenaza se materialice sus consecuencias no sean tan altas o desastrosas como en caso de que el riesgo no se minimice
- Transferirlo: Para este acción, y una vez identificado el riesgo la organización decide que a pesar de las medidas tomadas su probabilidad no se puede disminuir más, y que la organización no puede asumirlo, llegados a este punto estos riesgos se transfieren, para lo cual lo usual es usar alguna póliza de seguros que nos proteja en caso de que se materialice el riesgo, un ejemplo común de estos serían las pólizas contra incendios que tomas las organizaciones (a pesar de tener controles para minimizar los riesgos de incendios).
- Evitarlo: Una vez identificado el riesgo la organización decide eliminarlo, bien sea eliminado el activo de información susceptible al riesgo, elimina o cambio el proceso o servicio o elimina la amenaza o la vulnerabilidad que la permitía, esta acción es poco frecuente porque implica eliminar activos de información.

Una vez analizados los riesgos, se debe dar una verificación sobre la viabilidad tanto técnica como económica y operativa de las contramedidas o salvaguardas seleccionadas para mitigar los riesgos, es factible en esta etapa que las acciones sobre los riesgos cambien, debido a la imposibilidad o demora en realizar inversiones económicas, que las viabilidades técnicas no sean factibles, o que operativamente el impacto de implementar las salvaguardas o medidas de mitigación del riesgo sean muy altas (demoras adicionales en los procesos, contratación de gente, impacto en los tiempos de entrega, etc), de igual manera en los temas de costos es importante revisar que la inversión en las contramedidas no sea más alta que el valor de los activos, en cuyo caso no hace sentido

realizar estas inversiones y debemos realizar un cambio en la acción que se tomara sobre el riesgo identificado.

Con esta información clara y debidamente costeada en términos económicos y de recursos humanos y de tiempo, la Gerencia de Procesos y riesgos debe determinar los niveles de riesgo que la organización está dispuesta a asumir y sus costos asociados, con este panorama claro se deben determinar los controles a aplicar a los diferentes riesgos identificados

3.3 Valoración de los Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberadamente o accidentalmente con consecuencias para la organización. Incluye: información, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos financieros y recursos humanos.

De acuerdo con el apartado 1.7 “Sistemas de Información que dan soporte a la Organización” el inventario de los activos de la información queda reflejado en la siguiente tabla.

Tabla de Inventario de Activos

Ambito	Activo
Instalaciones	Centro de Procesamiento de Datos: Centro de Computo Principal
	Dirección de Infraestructura y Telecomunicaciones
	Sala Electrica, UPS y Plastas de Energia
Hardware	Servidores: HPNonStop, AS/400, srv1,srv2,srv3,srv4,srv5,srv6
	Equipos Escritorio, Portatiles, SmarthPhones
	Equipos de Comunicaciones: Cisco Catalys 7200
	Equipos de Seguridad Perimetral: Firewall Cisco ASA
	Central Telefonica: Alcatel 5500
Software Base	Windows Server 2012
	Windows Server 2008 R2
	AIX version 7.1
	OS/400 7.1
	Solaris 10

Aplicaciones	Bases de Datos: Oracle 11G
	Correo Electronico: Lotus Notes 8.5
	Antivirus: Symantec
	WebServer: Iplanet
	Sistema de Backups: Symantec Backup Exec
	IPS e IDS: Palo Alto Network
Datos	Información de Tarjetahabientes
	Codigo Fuente de Programas: Procesos de Canje y Compensación
	Registros de Actividad: Logs de software base y Aplicaciones
Red	Red de Datos:Ethernet
	Red de Telefonia: Ethernet (Voz IP)
	Acceso a Internet: Fibra Optica
Servicios	Internet
	Intranet
	Telefonia
Equipos Adicionales	Sistemas de Alimentación Interrumpida (UPS)
	Sistemas generadores de Energia
	Sistemas de aire acondicionado Ambiental y de Precision
	Equipos de control de temperatura y Ambiental
	Sistema de cableado electrico: Centro de procesamiento de datos
	Sistema de Cableado Electrico: Sede central
	Sistema de cableado de datos: Centro de procesamiento de datos (UTP cat 6)
	Sistema de cableado de datos: Sede Central (UTP Cat 5)
Personal	Administradores de Infraestructura
	Administradores de Telecomunicaciones
	Administradores de Bases de Datos
	Administradores de Aplicativos
	Administradores Funcionales
	Administradores de Seguridad Informática
	Director de Infraestructura y Telecomunicaciones
	Oficial de Seguridad de la Información (área de riesgos)
	Director de Sistemas 1 (Diseño y Desarrollo)
Soportes de Información	Discos Duros Servidores y estaciones de trabajo
	Cintas magneticas información de backups
	Unidades de Cd. DVD's, Memorias Extraibles

Tabla 2: Análisis de los Activos

Siguiendo la metodología vamos a definir unas tablas de valoración de activos con el fin de utilizarla sobre la tabla general de los activos de información.

Las escalas de valoración de los activos quedan definidas con las siguientes categorías despreciable, muy bajo, bajo, medio, alto y Muy alto, y se han definido unas abreviaturas para cada una de ellas con el fin de poder utilizarlas más adelante.

Valor de los activos		
Descripción	**Abreviatura**	**Valor**
Muy alto	MA	>100000
Alto	A	>40000 <100000
Medio	M	>9000 <40000
Bajo	B	>3000 <9000
Muy bajo	MB	>500 <3000
Despreciable	D	<500

Tabla 3: Clasificación del Valor de los Activos

En esta tabla quedan establecidos los rangos de valores de los activos de la información en las categorías respectivas, en donde un activo con valor de menos de 500 dólares para este ejercicio se puede considerar despreciable, y en donde un activo con valor mayor a 100000 dólares se considera un activo con un valor muy alto.

Elementos Claves del Sistema de la Organización											
				Categoría							
Id	Activo	Criticidad	Valor	Hardware	Software	Interfaces	Datos	Personal	Servicios	Misión
1	Switch Transaccional	Alta	Muy Alto	X	X		X		Servicio de Switch Transaccional	Autorizar o denegar las transacciones de los tarjetahabientes
2	Sistema Canje y Compensación	Alta	Alto	X	X		X		Servidor de Canje y Compensación	Relizar el proceso de Cnaje y Compensación entre los actores del negocio
3	Codigo Fuente	Alta	Muy Alto		X				Codigo fuentes de las apliaciones de negocio de la o	Administración componentes solución y funcionalidades de los productos
4	Equipos POS	Alta	Alto	X	X	X			Recepción y transmisión de transacciones de tarjeta	Captura y enrutamiento de las transacciones realizadas por los tarjetahabientes
5	Equipos de Telecomunicaciones	Alta	Alto	X	X				Transmisión de datos	Gestionar la transmisión de los datos generados en el negocio
6	Equipos de Seguridad Perimetral	Alta	Muy Alto	X	X	X			Servicios de Seguridad Perimetral	Portección de las redes de datos de accesos no autorizados
7	Servidor WEB de e-commerce	Medio	Alto	X	X				Servicios plataforma de E-commerce	Facilitar las compras en linea a los usuarios finales y comercios
8	Ambiente para Desarrollo	Alta	Alto	X	X		X		Facilitar el Desarrollo de software	Permitir el trabajo de los desarrolladores
9	Director de Infraestructura y Telecomunicaciones	Alta	Alto					X	Administración del área	Responsable de los componentes de la infraestructura y de las telecomunicaicones de los ambientes de pruebas, certificación y producción
10	Servidor de Correo Lotus	Medio	Alto	X	X		X		Servidor correo electronico de la organización	Intercambio de correo interno y externo
11	Desarrolladores de Software	Alta	Medio					X	Desarrollo software de la Organización	Implementar los desarrollos de software de la comañia
12	Servidor de EFT Server	Alta	Alto	X	X		X		Servidor de Intercambio de Archivos	Intercambio de archivos con los actores del proceso
13	Servidor Controlador de Dominio	Alta	Medio	X	X		X		Servidor de validación centralizada de usuarios	Autenticación centralizada y servicios de Directorio Activo
14	Servidor ERP	Medio	Medio	X	X		X		Servidor de Enterprise Resource Management	Servidor de administración centralizada de recursos empresariales
15	Servidor de Nomina	Medio	Medio	X	X		X		Servidor de Nomina	Servidor donde se gestiona la nomina de los colaboradores

Tabla 4: Elementos Claves del Sistema de la Organización

A continuación la valoración de las dimensiones de seguridad de los activos que incluyen aspectos como Autenticidad, Criticidad, Integridad, Disponibilidad y trazabilidad

Valoración Dimensiones de Seguridad de los Activos							
Ambito	Activo	Valor	Aspectos Criticos				
			A	C	I	D	T
Instalaciones	Centro de Procesamiento de Datos: Centro de Computo Principal	Muy Alto				10	
	Dirección de Infraestructura y Telecomunicaciones	Alto				7	
	Sala Electrica, UPS y Plantas de Energia	Muy Alto				10	
Hardware	Servidor HP NonStop	Muy Alto	10	10	10	10	10
	Servidor AS/400	Muy Alto	10	10	10	10	10
	Servidor EFT	Muy Alto	10	10	10	9	10
	Servidor E-commerce	Muy Alto	10	10	10	10	10
	Servidor E-commerce	Muy Alto	10	10	10	10	10
	Servidor ERP	Muy Alto	10	10	10	10	10
	Servidor Nomina	Muy Alto	10	10	10	10	10
	Servidor Directorio Activo	Muy Alto	10	10	10	10	9
	Servidor de Correo electrónico	Muy Alto	10	10	10	8	10
	Servidor Antivirus	Medio	7	6	7	6	7
	Servidor de Backups	Muy Alto	10	10	10	8	10
	Equipos Escritorio, Portatiles, SmarthPhones	Alto	8	6	7	7	7
	Equipos de Comunicaciones: Cisco Catalys 7200	Muy Alto	10	9	10	10	9
	Equipos de Seguridad Perimetral: Firewall Cisco ASA	Muy Alto	10	10	10	10	10
	Equipo de Seguridad Perimetral: Appliance de IDS e IPS	Alto	8	9	9	8	8
	Central Telefonica: Alcatel 5500	Medio	5	6	6	8	8
Aplicación	AIX version 7.1	Muy Alto	10	9	9	10	10
	OS/400 7.1	Muy Alto	10	9	9	10	10
	Sistemas Operativos: Windows Server 2008 R2	Muy Alto	10	9	8	10	10
	Sistema Operativo: Windows Server 2012	Muy Alto	10	9	8	10	10
	Sistema Operativo: Windows 7 Profesional	Alto	7	8	7	6	8
	Bases de Datos: Oracle 11G	Muy Alto	10	10	10	10	10
	Correo Electronico: Lotus Notes 8.5	Alto	9	8	8	7	8
	Antivirus: Symantec	Alto	9	6	8	6	8
	WebServer: Iplanet	Muy Alto	10	10	9	9	9
	Sistema de Backups: Symantec Backup Exec	Alto	8	8	8	6	8
	IPS e IDS: Palo Alto Network	Medio	8	6	8	6	6
Datos	Información de Tarjetahabientes	Muy Alto	10	10	10	10	10
	Codigo Fuente de Programas	Muy Alto	9	9	10	10	9
	Registros de Actividad: Logs de software base y Aplicaciones	Muy Alto	9	9	9	10	9
Red	Red de Datos:Ethernet	Muy Alto				10	
	Red de Telefonia: Ethernet (Voz IP)	Alto				8	
	Acceso a Internet: Fibra Optica	Muy Alto				10	
Servicios	Internet	Muy Alto				10	
	Intranet	Muy Alto				9	
	Telefonia	Muy Alto				10	
Equipos Adicionales	Sistemas de Alimentación Interrumpida (UPS)	Muy Alto				10	
	Sistemas generadores de Energia	Alto				8	
	Sistemas de aire acondicionado Ambiental y de Precision	Muy Alto				10	
	Equipos de control de temperatura y Ambiental	Alto				7	
	Sistema de cableado electrico: Centro de procesamiento de datos	Muy Alto				10	
	Sistema de Cableado Electrico: Sede central	Muy Alto				8	
	Sistema de cableado de datos: Centro de procesamiento de datos (UTP cat 6)	Muy Alto				10	
	Sistema de cableado de datos: Sede Central (UTP Cat 5)	Muy Alto				8	
Personal	Director de Infraestructura y Telecomunicaciones	Muy Alto		9		9	
	Administradores (Seguridad, Sistemas Operativos, Bases de Datos)	Muy Alto		10		9	
	Desarrolladores	Muy Alto		10		9	
	Director de Sistemas 1 (Diseño y Desarrollo)	Muy Alto		10		8	
	Proveedores	Muy Alto		10		8	
Soportes de Información	Discos Duros Servidores y estaciones de trabajo	Muy Alto	10	10	10	10	10
	Cintas magneticas información de backups	Muy Alto	9	7	10	7	10
	Unidades de Cd. DVD's, Memorias Extraibles	Alto		6	8	7	

Tabla 5: Valoración Dimensiones de Seguridad de los Activos

A continuación identificamos las amenazas que pueden sufrir nuestros activos de la información

Tabla de Identificación de Amenazas

Id	Amenaza	Fuente			Origen	Motivación	Acción
		Natural	Humana	Entorno			
1	Hurto del codigo Fuente		X		Competencia, empleados inconformes	Economica, causar daño a la compañía	Hurto del codigo fuente
2	Hurto de Hardware		X		Empleados inconformes, ladrones	Economica, causar daño a la compañía	Hurto de hardware (Unidades de POS)
3	Inundación	X			Origen natural (quebrada, lluvia torrencial) o falla de mantenimiento (tanque de reserva, tuberias)	Desastre natural	Inundación de la planta baja dañando todos los equipos
4	Terremoto	X			Origen natural	Desastre Natural	Probabilidad de Perdida de infraestrutura y de vidas humanas
5	Incendio	X			Fallas Electricas, factores ambientales	Desastre Natural o Motivación economica si es intencional	Probabilidad de Perdida de infraestrutura y de vidas humanas
6	Ejecución Software Malicioso			X	Actividades de los empleados	Economica	Ejecución de archivos con malware (virus, troyanos, spyware, adware, etc)
7	Acceso Fisico no Autorizado		X		Empleados inconformes, terceros	Economica, causar daño a la compañía	Ingreso indebido a las instalaciones
8	Acceso Logico no Autorizado		X		Empleados inconformes, terceros, Espionaje Industrial	Economica, errores no intencionados en los permisos	Ingreso indebido a las funcionalidades del programa, o a los datos almacenados en los sistemas
9	Incumplimiento Legal		X		Fallas Humanas	Desconocimiento, Causar daño a la compañía	No cumplir requisitos de ley
10	Indisponibilidad de recursos humanos		X		Bajas, vacaciones, abandono, enfermedad	Inclumplimiento de actividades laborales	Inasistencia del personal a laborar
11	Filtración de datos personales o tecnicos		X		Empleados inconformes	Economica, causar daño a la compañía	Revelar información privilegiada
12	Fallas en las Telecomunicaciones		X	X	Fallas en los equipos o enlaces de Telecomunicaciones	Fallas tecnicas o humanas, sabotage, robo	Imposibilidad de prestar los servicios

Tabla 6: Tabla de Identificación de Amenazas

Para continuar con nuestro proceso de valoración de riesgos es necesario definir una tabla en donde estén estimadas las frecuencias de ocurrencias de las amenazas con los valores calculados sobre un marco de tiempo de un año.

Frecuencia			
Descripción	Abreviatura	Rango	Valor
Extremadamente frecuente	EF	1 Vez al dia	1.000000
Muy frecuente	MF	1 vez cada dos semanas Valor 26/365	0.071233
Frecuente	F	1 vez cada dos meses Valor 6/365	0.016438
Poco Frecuente	PF	1 vez cada seis meses Valor 2/365	0.005479
Muy poco frecuente	MPF	1 vez al año Valor 1/365	0.002739
Despreciable	D	< 1 vez cada 3 años	0.000913

Tabla 7: Cálculo de Frecuencia

En la tabla de frecuencias, tenemos calculado los valores de despreciable cuando la frecuencia de ocurrencia de la amenaza es menor a una vez cada tres años, y extremadamente frecuente cuando la ocurrencia es una vez por día.

La siguiente tabla de impacto valora de manera cuantitativa el valor del impacto de ocurrencia de las amenazas

Impacto		
Descripción	**Abreviatura**	**Valor**
Critico	C	100%
Alto	A	75%
Medio	M	25%
Bajo	B	10%

Tabla 8: Tabla de Impacto

Variación Impacto/Vulnerabilidad		
Descripción	**Abreviatura**	**Valor**
Alta	A	95%
Media	M	75%
Baja	B	25%
Despreciable	D	10%

Tabla 9: Disminución del Impacto o la Frecuencia

Con la tabla 9, la organización estima que en caso de utilizar la mejor medida de seguridad posible para determinado riesgo, ésta le ayudará a reducir su riesgo inicial en un 95%, y así para cada uno de los niveles que se han establecido

El valor del riesgo entonces lo calculamos con el valor del activo (tabla 3), la frecuencia (tabla 7), y el impacto (Tabla 8)

Riesgos	Centro de Procesamiento		Dir Inf y Teleco		Sala Electrica, UPS y Planta de Energia		Swith Transaccional	
Valor del Activo		600000		150000		250000		500000
Hurto Codigo Fuente	0.005479	100%	0.002739	100%	0.002739	100%		
		3287.4		410.85		684.75		0
Hurto de Hardware	0.005479	100%	0.002739	100%	0.002739	100%	0.002739	100%
		3287.4		410.85		684.75		1369.5
Inundación	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		547.8		136.95		228.25		456.5
Terremoto	0.000913	75%	0.000913	75%	0.000913	75%	0.000913	75%
		410.85		102.7125		171.1875		342.375
Incendio	0.000913	75%	0.000913	75%	0.000913	75%	0.000913	75%
		410.85		102.7125		171.1875		342.375
Ejecución Software Malicioso	0.005479	100%	0.005479	100%	0.000913	100%		
		3287.4		821.85		228.25		0
Acceso Fisico no autorizado	0.005479	100%	0.005479	100%	0.000913	100%	0.000913	100%
		3287.4		821.85		228.25		456.5
Acceso Logico no Autorizado	0.002739	100%	0.002739	100%	0.000913	100%	0.000913	100%
		1643.4		410.85		228.25		456.5
Incumplimiento Legal								
Indisponibilidad de Recursos Humanos	0.005479	75%	0.005479	75%	0.002739	10%	0.002739	10%
		2465.55		616.3875		68.475		136.95
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	100%	0.002739	10%	0.002739	100%
		1643.4		410.85		68.475		1369.5
Fallas en las Telecomunicaciones	0.071233	100%	0.071233	100%	0.002739	10%	0.002739	100%
		42739.8		10684.95		68.475		1369.5
Riesgo anual por activo		**63011.25**		**14930.81**		**2830.30**		**6299.70**

Riesgos	Sistema Canje y Compensación		Servidor de EFT		Servidor Web e-commerce		Servidor Web e-commerce DB	
Valor del Activo		200000		18000		15000		15000
Hurto Codigo Fuente								
		0		0		0		0
Hurto de Hardware	0.000913	100%	0.002739	100%	0.000913	100%	0.000913	100%
		182.6		49.302		13.695		13.695
Inundación	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		182.6		16.434		13.695		13.695
Terremoto	0.000913	75%	0.000913	100%	0.000913	100%	0.000913	100%
		136.95		16.434		13.695		13.695
Incendio	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		182.6		16.434		13.695		13.695
Ejecución Software Malicioso								
		0		0		0		0
Acceso Fisico no autorizado	0.000913	100%	0.002739	100%	0.002739	100%	0.002739	100%
		182.6		49.302		41.085		41.085
Acceso Logico no Autorizado	0.000913	100%	0.002739	100%	0.002739	100%	0.002739	100%
		182.6		49.302		41.085		41.085
Incumplimiento Legal								
				0		0		0
Indisponibilidad de Recursos Humanos	0.002739	10%	0.002739	10%	0.002739	10%	0.002739	10%
		54.78		4.9302		4.1085		4.1085
Filtración de Datos personales o Tecnicos	0.000913	100%	0.002739	100%	0.002739	100%	0.002739	100%
		182.6		49.302		41.085		41.085
Fallas en las Telecomunicaciones	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
		547.8		49.302		41.085		41.085
Riesgo anual por activo		**1835.13**		**300.74**		**223.23**		**223.23**

Riesgos	Servidor Directorio Activo		Servidor de ERP		Servidor de Nomina		Servidor Correo	
Valor del Activo	12000		18000		12000		120000	
Hurto Codigo Fuente								
	0		0		0		0	
Hurto de Hardware	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
	32.868		49.302		32.868		328.68	
Inundación	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
	10.956		16.434		10.956		109.56	
Terremoto	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
	10.956		16.434		10.956		109.56	
Incendio	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
	10.956		16.434		10.956		109.56	
Ejecución Software Malicioso								
	0		0		0		0	
Acceso Fisico no autorizado	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
	32.868		49.302		32.868		328.68	
Acceso Logico no Autorizado	0.002739	100%	0.002739	100%	0.002739	100%		
	32.868		49.302		32.868		0	
Incumplimiento Legal								
	0		0		0		0	
Indisponibilidad de Recursos Humanos	0.002739	10%	0.002739	10%	0.002739	10%		
	3.2868		4.9302		3.2868		0	
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
	32.868		49.302		32.868		328.68	
Fallas en las Telecomunicaciones	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
	32.868		49.302		32.868		328.68	
Riesgo anual por activo		**200.49**		**300.74**		**200.49**		**1643.40**

Riesgos	Servidor de Antivirus		Servidor Backups		Servidor I-Planet		Equipos POS	
Valor del Activo	12000		18000		18000		80000	
Hurto Codigo Fuente							0.002739	100%
	0		0		0		219.12	
Hurto de Hardware	0.002739	100%	0.002739	100%	0.002739	100%	0.005479	75%
	32.868		49.302		49.302		328.74	
Inundación	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
	10.956		16.434		16.434		73.04	
Terremoto	0.000913	100%	0.000913	100%	0.000913	100%	0.002739	100%
	10.956		16.434		16.434		219.12	
Incendio	0.000913	100%	0.000913	100%	0.000913	100%	0.002739	100%
	10.956		16.434		16.434		219.12	
Ejecución Software Malicioso							0.000913	100%
	0		0		0		73.04	
Acceso Fisico no autorizado	0.002739	100%	0.002739	100%	0.002739	100%	0.005479	75%
	32.868		49.302		49.302		328.74	
Acceso Logico no Autorizado	0.002739	100%	0.002739	100%	0.002739	100%	0.000913	100%
	32.868		49.302		49.302		73.04	
Incumplimiento Legal								
	0		0		0			
Indisponibilidad de Recursos Humanos	0.002739	10%	0.002739	10%	0.002739	10%	0.002739	10%
	3.2868		4.9302		4.9302		21.912	
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	100%	0.002739	100%	0.000913	100%
	32.868		49.302		49.302		73.04	
Fallas en las Telecomunicaciones	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
	32.868		49.302		49.302		219.12	
Riesgo anual por activo		**200.49**		**300.74**		**300.74**		**1848.03**

Riesgos	Equipos Telecomunicaciones		Equipos escritorios, portatiles, Smartphones		Equipos Seguridad Perimetral: Firewall		Equipos Seguridad Perimetral: IPS e IDS	
Valor del Activo	35000		600000		140000		95000	
Hurto Codigo Fuente								
	0		0		0		0	
Hurto de Hardware	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
	31.955		547.8		127.82		86.735	
Inundación	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
	31.955		547.8		127.82		86.735	
Terremoto	0.000913	75%	0.000913	75%	0.000913	100%	0.000913	100%
	23.96625		410.85		127.82		86.735	
Incendio	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
	31.955		547.8		127.82		86.735	
Ejecución Software Malicioso	0.005479	100%	0.005479	100%	0.002739	100%	0.002739	100%
	191.765		3287.4		383.46		260.205	
Acceso Fisico no autorizado	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
	95.865		1643.4		383.46		260.205	
Acceso Logico no Autorizado	0.002739	100%	0.005479	100%	0.002739	100%	0.002739	100%
	95.865		3287.4		383.46		260.205	
Incumplimiento Legal					0.002739	100%		
	0		0		383.46		0	
Indisponibilidad de Recursos Humanos			0.002739	10%	0.002739	10%	0.002739	10%
	0		164.34		38.346		26.0205	
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	100%	0.000913	100%	0.000913	100%
	95.865		1643.4		127.82		86.735	
Fallas en las Telecomunicaciones	0.002739	100%	0.002739	75%	0.002739	100%	0.002739	100%
	95.865		1232.55		383.46		260.205	
Riesgo anual por activo		**695.06**		**13312.74**		**2594.75**		**1500.52**

Riesgos	Central Telefonica		SO HP NonStop		OS 400		AIX 7.1	
Valor del Activo	40000		300000		60000		12000	
Hurto Codigo Fuente			0.000913	100%	0.000913	100%	0.000913	100%
	0		273.9		54.78		10.956	
Hurto de Hardware	0.000913	100%						
	36.52							
Inundación	0.000913	100%						
	36.52							
Terremoto	0.000913	100%						
	36.52							
Incendio	0.000913	100%						
	36.52							
Ejecución Software Malicioso	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
	109.56		821.7		164.34		32.868	
Acceso Fisico no autorizado	0.002739	100%						
	109.56		0		0		0	
Acceso Logico no Autorizado	0.002739	100%	0.000913	100%	0.000913	100%	0.000913	100%
	109.56		273.9		54.78		10.956	
Incumplimiento Legal								
	0		0		0		0	
Indisponibilidad de Recursos Humanos	0.002739	10%	0.005479	75%	0.005479	75%	0.005479	75%
	10.956		1232.775		246.555		49.311	
Filtración de Datos personales o Tecnicos	0.000913	10%	0.002739	100%	0.002739	100%	0.002739	100%
	3.652		821.7		164.34		32.868	
Fallas en las Telecomunicaciones	0.002739	100%	0.005479	100%	0.005479	100%	0.005479	100%
	109.56		1643.7		328.74		65.748	
Riesgo anual por activo		**598.93**		**5067.68**		**1013.54**		**202.71**

Riesgos	Windows Server 2012		Windows 7 Profesional		Oracle 11G		Lotus Notes 8.5	
Valor del Activo		12000		12000		12000		12000
Hurto Codigo Fuente	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		10.956		10.956		10.956		10.956
Hurto de Hardware								
Inundación								
Terremoto								
Incendio								
Ejecución Software Malicioso	0.002739	100%	0.005479	100%	0.002739	100%	0.002739	100%
		32.868		65.748		32.868		32.868
Acceso Fisico no autorizado								
		0		0		0		0
Acceso Logico no Autorizado	0.000913	100%	0.005479	100%	0.000913	100%	0.000913	100%
		10.956		65.748		10.956		10.956
Incumplimiento Legal								
		0		0		0		0
Indisponibilidad de Recursos Humanos	0.005479	75%	0.005479	75%	0.005479	75%	0.005479	75%
		49.311		49.311		49.311		49.311
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	75%	0.002739	100%	0.002739	100%
		32.868		24.651		32.868		32.868
Fallas en las Telecomunicaciones	0.005479	75%	0.005479	25%	0.005479	75%	0.005479	75%
		49.311		16.437		49.311		49.311
Riesgo anual por activo		**186.27**		**232.85**		**186.27**		**186.27**

Riesgos	Antivirus Symantec		Symantec Backup EXEC		IDS/IPS Palo Alto		Datos de Tarjetahabientes	
Valor del Activo		12000		12000		12000		400000
Hurto Codigo Fuente	0.000913	100%	0.000913	100%	0.000913	100%		
		10.956		10.956		10.956		
Hurto de Hardware								
Inundación								
Terremoto								
Incendio								
Ejecución Software Malicioso	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
		32.868		32.868		32.868		1095.6
Acceso Fisico no autorizado								
		0		0		0		0
Acceso Logico no Autorizado	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		10.956		10.956		10.956		365.2
Incumplimiento Legal								
		0		0		0		0
Indisponibilidad de Recursos Humanos	0.005479	75%	0.005479	75%	0.005479	25%	0.005479	75%
		49.311		49.311		16.437		1643.7
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	100%	0.002739	75%	0.002739	100%
		32.868		32.868		24.651		1095.6
Fallas en las Telecomunicaciones	0.005479	75%	0.005479	100%	0.005479	100%	0.005479	100%
		49.311		65.748		65.748		2191.6
Riesgo anual por activo		**186.27**		**202.71**		**161.62**		**6391.70**

Riesgos	Codigo Fuente de Programas		Registros de Actividad		Red de Datos		Telefonia	
Valor del Activo		180000		12000		120000		150000
Hurto Codigo Fuente	0.002739	100%						
		493.02						
Hurto de Hardware								
Inundación					0.000913	100%	0.000913	100%
						109.56		136.95
Terremoto					0.000913	100%	0.000913	100%
						109.56		136.95
Incendio					0.000913	100%	0.000913	100%
						109.56		136.95
Ejecución Software Malicioso	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	25%
		493.02		32.868		328.68		102.7125
Acceso Fisico no autorizado								
		0						
Acceso Logico no Autorizado	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		164.34		10.956		109.56		136.95
Incumplimiento Legal								
		0		0				
Indisponibilidad de Recursos Humanos	0.005479	25%	0.005479	25%	0.002739	10%	0.002739	25%
		246.555		16.437		32.868		102.7125
Filtración de Datos personales o Tecnicos	0.002739	75%	0.002739	75%	0.002739	75%	0.002739	100%
		369.765		24.651		246.51		410.85
Fallas en las Telecomunicaciones	0.005479	100%	0.005479	100%	0.002739	100%	0.002739	100%
		986.22		65.748		328.68		410.85
Riesgo anual por activo		**2752.92**		**150.66**		**1374.98**		**1574.93**

Riesgos	Internet		Sistemas de UPS		Sistemas de Generación de Energia		Aires Acondicionados	
Valor del Activo		150000		120000		45000		90000
Hurto Codigo Fuente								
Hurto de Hardware			0.000913	100%	0.000913	100%	0.000913	100%
				109.56		41.085		82.17
Inundación	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		136.95		109.56		41.085		82.17
Terremoto	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		136.95		109.56		41.085		82.17
Incendio	0.000913	100%	0.000913	100%	0.000913	100%	0.000913	100%
		136.95		109.56		41.085		82.17
Ejecución Software Malicioso	0.071233	100%	0.071233	100%			0.071233	100%
		10684.95		8547.96				6410.97
Acceso Fisico no autorizado			0.002739	100%	0.002739	100%	0.002739	100%
				328.68		123.255		246.51
Acceso Logico no Autorizado	0.071233	100%	0.071233	100%			0.071233	100%
		10684.95		8547.96				6410.97
Incumplimiento Legal								
Indisponibilidad de Recursos Humanos	0.002739	25%	0.002739	25%	0.002739	25%	0.002739	25%
		102.7125		82.17		30.81375		61.6275
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	25%	0.002739	100%	0.002739	100%
		410.85		82.17		123.255		246.51
Fallas en las Telecomunicaciones	0.002739	100%	0.002739	25%			0.002739	100%
		410.85		82.17				246.51
Riesgo anual por activo		**22705.16**		**18109.35**		**441.66**		**13951.78**

Riesgos	Sistema de Cableado electrico		Director de Inf y Teleco		Administradores		Desarrolladores	
Valor del Activo		60000		50000		35000		32000
Hurto Codigo Fuente								
				0		0		0
Hurto de Hardware	0.000913	100%						
		54.78		0		0		0
Inundación	0.000913	100%						
		54.78		0		0		0
Terremoto	0.000913	100%	0.000913	100%				
		54.78		45.65		0		0
Incendio	0.000913	100%	0.000913	100%				
		54.78		0		0		0
Ejecución Software Malicioso								
				0		0		0
Acceso Fisico no autorizado	0.002739	100%						
		164.34		0		0		0
Acceso Logico no Autorizado								
				0		0		0
Incumplimiento Legal					0.002739	100%	0.002739	100%
						95.865		87.648
Indisponibilidad de Recursos Humanos	0.002739	25%	0.002739	100%	0.002739	100%	0.002739	100%
		41.085		136.95		95.865		87.648
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%
		164.34		136.95		95.865		87.648
Fallas en las Telecomunicaciones								
				0		0		0
Riesgo anual por activo		**588.89**		**319.55**		**287.60**		**262.94**

Riesgos	Director de Sistemas 1		Discos Duros Servidores y estaciones		Cintas Magneticas		Unidades de Cd's , DVD's, Memorias		
Valor del Activo		50000		60000		60000		12000	Año
Hurto Codigo Fuente			0.000913	100%					
		0		54.78					**5566.25**
Hurto de Hardware			0.000913	100%	0.000913	100%	0.000913	100%	
		0		54.78		54.78		10.956	**8154.66**
Inundación			0.000913	100%	0.000913	100%	0.000913	100%	
		0		54.78		54.78		10.956	**3483.10**
Terremoto			0.000913	100%	0.000913	100%	0.000913	100%	
		0		54.78		54.78		10.956	**3141.86**
Incendio			0.000913	100%	0.000913	100%	0.000913	100%	
		0		54.78		54.78		10.956	**3286.80**
Ejecución Software Malicioso									
		0		0		0		0	**37621.55**
Acceso Fisico no autorizado			0.002739	100%	0.002739	100%	0.002739	100%	
		0		164.34		164.34		32.868	**9728.83**
Acceso Logico no Autorizado									
		0						0	**34411.12**
Incumplimiento Legal	0.002739	100%			0.002739	10%			
		136.95				16.434		0	**720.36**
Indisponibilidad de Recursos Humanos	0.002739	100%			0.002739	25%	0.002739	100%	
		136.95				41.085		32.868	**8374.51**
Filtración de Datos personales o Tecnicos	0.002739	100%	0.002739	100%	0.002739	100%	0.002739	100%	
		136.95		164.34		164.34		32.868	**11638.01**
Fallas en las Telecomunicaciones									
		0		0		0		0	**65523.94**
Riesgo anual por activo		**410.85**		**602.58**		**605.32**		**142.43**	**191650.98**

Tabla 10: Valoración del Riesgo

3.4 Plan de Tratamiento del Riesgo

Una vez establecidos los niveles de riesgo para los diferentes activos, se debe establecer las medidas de protección, salvaguardas o contramedidas que se deben implementar para cada uno de los activos en función del impacto que pueda representar la materialización de la amenaza.

Amenaza	Activo	Controles
Hurto del codigo Fuente	Switch Transaccional Sistema de Canje y Compensación Codigo Fuente Equipos POS Servidor Web E-commerce Ambiente de Desarrollo	Se enviaran los logs de acceso de todas las plataformas a un sistema centralizado que facilitara su revisión Se implementaran sistemas de monitoreo de archivos en las rutas en donde esta el codigo fuente Se firmaran contratos de confidencialidad con los desarrolladores interno y/o externos del codigo fuente Se implementara un IDS/IPS (Sistema de Detección de Intrusos/Sistema de Prevención de Intrusos) para detectar y prevenir intentos de acceso indebidos a los sistemas Se definira e implementara un procedimiento de atención de Incidentes de Seguridad
Hurto de Hardware	Swith Transaccional Sistema de Canje y Compensación Equipos POS Equipos Telecomunicaciones Equipos Seguridad Perimetral Servidor Web e-commerce Servidor de Lotus Notes Servidor de EFT Controlador de Dominio Servidor de ERP Servidor de Nomina	Los rack en donde estan los servidores deberan estar siempre con llaves y estas deben estar en la caja fuerte del centro de computo El retiro de equipo y/o partes debe ser realizado solo por personal autorizado y controlado por medio de ordenes de salidad debidamente gestionadas y formadas Todos los servidores contaran con software de monitoreo que avisara acerca del cambio en sus caracteristicas de hardware y/o software Se llevara un inventario estricto de los equipos POS y su almacenaje, alistamiento y entrega se supervisara de manera especial

Inundación	Swith Transaccional Sistema de Canje y Compensación Equipos POS Equipos Telecomunicaciones Equipos Seguridad Perimetral Servidor Web e-commerce Servidor de Lotus Notes Servidor de EFT Controlador de Dominio Servidor de ERP Servidor de Nomina	El Centro de computo se ubicara en el piso cuarto en donde el riesgo de una inundación es menor Se contratarán polizas de seguros que protegan los activos de la información del riesgo de incendio Se eliminaran todas las tuberias de agua del centro de computo, sala electrica, UPS's y plantas de energia y sus sitios cercanos Se instalaran en los acceso de centro de computo, sala electrica, cuarto de UPS's y planta de energia puertas selladas que impidan la filtración de Agua
Terremoto	Instalaciones Hardware Equipo Adicional Personal	Se contratará una poliza de seguros que cubra las instalaciones, el hardware y el equipo adicional del riesgo de un terremoto Se crearan comites de atención de desastres en donde se realicen simulacros de casos de terremoto
Incendio	Instalaciones Hardware Equipo Adicional Personal	Se contratará una poliza de seguros que cubra las instalaciones, el hardware y el equipo adicional del riesgo de un terremoto Se crearan comites de antención de desastres en donde se realicen simulacros de casos de Incendio Se instalaran sistemas de detección y extinción de incendios e instalarán extintitores en los sitios que se requieran
Ejecución Software Malicioso	Swith Transaccional Sistema de Canje y Compensación Equipos POS Equipos Telecomunicaciones Equipos Seguridad Perimetral Servidor Web e-commerce Servidor de Lotus Notes Servidor de EFT Controlador de Dominio Servidor de ERP Servidor de Nomina	Se implementara un IDS/IPS (Sistema de Detección de Intrusos/Sistema de Prevención de Intrusos) para detectar y prevenir software malicioso Se implementara un sistema de HIPS de host en cada uno de los servidores de la red Se desarrollará e implementará un plan de continuidad del negocio
Acceso Fisico no Autorizado	Instalaciones Servidores	Se implementará un sistema de acceso biometrico para el centro de computo y el área de tecnologia Se establecerá un procedimiento de acceso con registro de bitacora para el ingreso controlado a la sala electrica, UPS y Plantas de Energia Los servidores deben estar en el centro de computo con estrictos controles fisicos de acceso y en los rack bajo llave Se contratara soporte tecnico 7 x 24 en las diferentes plataformas para mejorar la disponibilidad de los sistemas
Acceso Logico no Autorizado	Swith Transaccional Sistema de Canje y Compensación Equipos POS Equipos Telecomunicaciones Equipos Seguridad Perimetral Servidor Web e-commerce Servidor de Lotus Notes Servidor de EFT Controlador de Dominio Servidor de ERP Servidor de Nomina	Se implementará un SIEM (Security Information and Event Management) que facilitara la centralización y monitoreo basado en los logs Para proteger el segmento de servidores se instalara un segundo firewall interno Para proter el segmento de servidores se instalara un sensor del IDS Sistema de Detección de Intrusos Se cambiaran los usuarios de acceso definidos por default por unos personalizados Las claves de administración de todos los elementos de infraestructura se guardaran en un caja de seguridad en sobre sellado Se estableceran procedimientos de cambios de contraseñas (complejas) para usuarios administradores Se establecera un procedimiento formal de analisis de vulnerabilidades con una herramienta dedicada a este servicio Se contrataran servicios de hacking etico para evaluar las oportunidades de mejora en las configuraciones de los diferentes componentes Se implementara una solución de NAC para evitar los intentos de escucha o sniffing de información en la red y las conexiones no autorizadas
Incumplimiento Legal	Swith Transaccional Sistema de Canje y Compensación Equipos POS	Se revisaran los contratos con los bancos y se estableceran claramente los niveles de servicio con ellos Se contratarán polizas de seguros que cubran los riesgos en caso de incumplimiento de los SLA's Se revisaran los contratos establecidos con los comercios para los niveles de servicio de los POS
Indisponibilidad de recursos humanos	Personal	Se documentarán las funciones de manera detallada para todo el personal de TI Para los cargos de mayor relevancia se establecera personal de respaldo que pueda cubrir al titular en casos de ausencia Los proyectos de desarrollo deberan contar con información documentada y actualizada acerca de su evolución para facilitar su entendimiento
Filtración de datos personales o tecnicos	Swith Transaccional Sistema de Canje y Compensación Equipos POS	Se estableceran procedimientos de configuración segura para todos los componentes de la infraestructura, guías de hardening para todos los elementos de la infraestructura Se implementara un sistema de Data Loss Prevención que protega los sistemas sensibles de perdidas deliberadas o accidentales de datos Se cifraran todos los datos desde el POS hasta el Switch Transaccional utilizando algoritmos fuertes de cifrado
Fallas en Telecomunicaciones	Swith Transaccional Sistema de Canje y Compensación Equipos POS Internet Intranet	Se contratarán canales de comunicaciones redundantes donde las condiciones del negocio lo permitan Se implementarán equipos de telecomunicaciones redundantes para atender las conexiones provenientes de los enlaces principales y de backup

Tabla 11: Plan de tratamiento del Riesgo

En la tabla de tratamiento del riesgo vemos la siguiente información: una columna con las amenazas identificadas para los activos, una columna donde están los activos que son susceptibles a la amenaza identificada y una tercera columna en donde están identificados los controles que aplican para mitigar la amenaza sobre los activos.

Algunos de los controles propuestos en razón a su naturaleza pueden ayudar en la mitigación de varias de las amenazas y servir para proteger varios de los activos, como puede ser el caso de la implementación de una solución de SIEM que permitirá monitorear los logs de varios de los activos

3.5 Riesgo Residual

A continuación detallaremos el nivel de riesgo residual, que son los riesgos remanentes que existes tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información, para ello la organización determina que la aplicación del mejor o mejores controles para mitigar un riesgo aporta una disminución del mismo en un 90% en promedio, el valor restante deberá ser asumido por la organización en cada uno de los activos.

A continuación se anexa la tabla de los activos con los valores calculados de los riesgos y las amenazas y una columna en donde se calcula el porcentaje de reducción de los riesgos, el valor calculado nos da el riesgo residual por activo sobre el cual la organización deberá tomar las decisiones del caso.

Tabla de Calculo de Riesgo Residual

Amenazas / Activos	Hurto Codigo Fuente	Hurto de Hardware	Inundación	Terremoto	Incendio	Ejecución Software Malicioso	Acceso Físico no autorizado	Acceso Logico no Autorizado	Incumplimiento Legal	Indisponibilidad de Recursos Humano	Filtración de Datos personales o Tecnic	Fallas en las Telecomunicaciones	Totales	**Reducción Riesgo Luego de Controles**	Riesgo Residual
Centro de Procesamiento de Datos: Centro de Computo Principal	3287.40	3287.40	547.80	410.85	410.85	3287.40	3287.40	1643.40	0.00	2465.55	1643.40	42739.80	63011.25	90%	6301.13
Dirección de Infraestructura y Telecomunicaciones	410.85	410.85	136.95	102.71	102.71	821.85	821.85	410.85	0.00	616.39	410.85	10684.95	14930.81	90%	1493.08
Sala Electrica, UPS y Plantas de Energia	684.75	684.75	228.25	171.19	171.19	228.25	228.25	228.25	0.00	68.48	68.48	68.48	2830.30	90%	283.03
Servidor HP NonStop	0.00	1369.50	456.50	342.38	342.38	0.00	456.50	456.50	0.00	136.95	1369.50	1369.50	6299.70	95%	314.99
Servidor AS/400	0.00	182.60	182.60	136.95	182.60	0.00	182.60	182.60	0.00	54.78	182.60	547.80	1835.13	95%	91.76
Servidor EFT	0.00	49.30	16.43	16.43	16.43	0.00	49.30	49.30	0.00	4.93	49.30	49.30	300.74	90%	30.07
Servidor E-commerce Web	0.00	13.70	13.70	13.70	13.70	0.00	41.09	41.09	0.00	4.11	41.09	41.09	223.23	90%	22.32
Servidor E-commerce DB	0.00	13.70	13.70	13.70	13.70	0.00	41.09	41.09	0.00	4.11	41.09	41.09	223.23	90%	22.32
Servidor Directorio Activo	0.00	32.87	10.96	10.96	10.96	0.00	32.87	32.87	0.00	3.29	32.87	32.87	200.49	90%	20.05
Servidor ERP	0.00	49.30	16.43	16.43	16.43	0.00	49.30	49.30	0.00	4.93	49.30	49.30	300.74	90%	30.07
Servidor Nomina	0.00	32.87	10.96	10.96	10.96	0.00	32.87	32.87	0.00	3.29	32.87	32.87	200.49	90%	20.05
Servidor de Correo electrónico	0.00	328.68	109.56	109.56	109.56	0.00	328.68	0.00	0.00	0.00	328.68	328.68	1643.40	90%	164.34
Servidor Antivirus	0.00	32.87	10.96	10.96	10.96	0.00	32.87	32.87	0.00	3.29	32.87	32.87	200.49	90%	20.05
Servidor de Backups	0.00	49.30	16.43	16.43	16.43	0.00	49.30	49.30	0.00	4.93	49.30	49.30	300.74	90%	30.07
Servidor I-Planet	0.00	49.30	16.43	16.43	16.43	0.00	49.30	49.30	0.00	4.93	49.30	49.30	300.74	90%	30.07
Equipos POS	219.12	328.74	73.04	219.12	219.12	73.04	328.74	73.04	0.00	21.91	73.04	219.12	1848.03	90%	184.80
Equipos de Telecomunicaciones: Cisco Catalys 7200	0.00	31.96	31.96	23.97	31.96	191.77	95.87	95.87	0.00	0.00	95.87	95.87	695.06	90%	69.51
Equipos de escritotrio, portatiles y SmartPhones	0.00	547.80	547.80	410.85	547.80	3287.40	1643.40	3287.40	0.00	164.34	1643.40	1232.55	13312.74	90%	1331.27
Equipos de Seguridad Perimetral: Firewall Cisco ASA	0.00	127.82	127.82	127.82	127.82	383.46	383.46	383.46	383.46	38.35	127.82	383.46	2594.75	90%	259.47
Equipo de Seguridad Perimetral: Appliance de IDS e IPS	0.00	86.74	86.74	86.74	86.74	260.21	260.21	260.21	0.00	26.02	86.74	260.21	1500.52	90%	150.05
Central Telefonica: Alcatel 5500	0.00	36.52	36.52	36.52	36.52	109.56	109.56	109.56	0.00	10.96	3.65	109.56	598.93	90%	59.89
SO. HP NonStop	273.90	0.00	0.00	0.00	0.00	821.70	0.00	273.90	0.00	1232.78	821.70	1643.70	5067.68	90%	506.77
OS/400 7.1	54.78	0.00	0.00	0.00	0.00	164.34	0.00	54.78	0.00	246.56	164.34	328.74	1013.54	90%	101.35
AIX 7.1	10.96	0.00	0.00	0.00	0.00	32.87	0.00	10.96	0.00	49.31	32.87	65.75	202.71	90%	20.27
Sistema Operativo: Windows Server 2012	10.96	0.00	0.00	0.00	0.00	32.87	0.00	10.96	0.00	49.31	32.87	49.31	186.27	90%	18.63
Sistema Operativo: Windows 7 Profesional	10.96	0.00	0.00	0.00	0.00	65.75	0.00	65.75	0.00	49.31	24.65	16.44	232.85	90%	23.29
Bases de Datos: Oracle 11G	10.96	0.00	0.00	0.00	0.00	32.87	0.00	10.96	0.00	49.31	32.87	49.31	186.27	90%	18.63
Correo Electronico: Lotus Notes 8.5	10.96	0.00	0.00	0.00	0.00	32.87	0.00	10.96	0.00	49.31	32.87	49.31	186.27	90%	18.63
Antivirus: Symantec	10.96	0.00	0.00	0.00	0.00	32.87	0.00	10.96	0.00	49.31	32.87	32.87	169.83	90%	16.98
Sistema de Backups: Symantec Backup Exec	10.96	0.00	0.00	0.00	0.00	32.87	0.00	10.96	0.00	49.31	32.87	65.75	202.71	90%	20.27
IPS e IDS: Palo Alto Network	10.96	0.00	0.00	0.00	0.00	32.87	0.00	10.96	0.00	16.44	24.65	65.75	161.62	90%	16.16
Información de Tarjetahabientes	0.00	0.00	0.00	0.00	0.00	1095.60	0.00	365.20	0.00	1643.70	1095.60	2191.60	6391.70	90%	639.17
Codigo Fuente de Programas	493.02	0.00	0.00	0.00	0.00	493.02	0.00	164.34	0.00	246.56	369.77	986.22	2752.92	90%	275.29
Registros de Actividad: Logs de software base y Aplicaciones	0.00	0.00	0.00	0.00	0.00	32.87	0.00	10.96	0.00	16.44	24.65	65.75	150.66	90%	15.07
Red de Datos:Ethernet	0.00	0.00	109.56	109.56	109.56	328.68	0.00	109.56	0.00	32.87	246.51	328.68	1374.98	90%	137.50
Red de Telefonia: Ethernet (Voz IP)	0.00	0.00	136.95	136.95	136.95	102.71	0.00	136.95	0.00	102.71	410.85	410.85	1574.93	90%	157.49
Acceso a Internet: Fibra Optica	0.00	0.00	136.95	136.95	136.95	10684.95	0.00	10684.95	0.00	102.71	410.85	410.85	22705.16	90%	2270.52
Sistemas de Alimentación Interrumpida (UPS)	0.00	109.56	109.56	109.56	109.56	8547.96	328.68	8547.96	0.00	82.17	82.17	82.17	18109.35	90%	1810.94
Sistemas generadores de Energia	0.00	41.09	41.09	41.09	41.09	0.00	123.26	0.00	0.00	30.81	123.26	0.00	441.66	90%	44.17
Sistemas de aire acondicionado Ambiental y de Precision	0.00	82.17	82.17	82.17	82.17	6410.97	246.51	6410.97	0.00	61.63	246.51	246.51	13951.78	90%	1395.18
Sistema de Cableado Electrico	0.00	54.78	54.78	54.78	54.78	0.00	164.34	0.00	0.00	41.09	164.34	0.00	588.89	90%	58.89
Director de Infraestructura y Telecomunicaciones	0.00	0.00	0.00	45.65	0.00	0.00	0.00	0.00	0.00	136.95	136.95	0.00	319.55	90%	31.96
Administradores (Seguridad, Sistemas Operativos, Bases de Datos)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	95.87	95.87	95.87	0.00	287.60	90%	28.76
Desarrolladores	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	87.65	87.65	87.65	0.00	262.94	90%	26.29
Director de Sistemas 1 (Diseño y Desarrollo)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	136.95	136.95	136.95	0.00	410.85	90%	41.09
Discos Duros Servidores y estaciones de trabajo	54.78	54.78	54.78	54.78	54.78	0.00	164.34	0.00	0.00	0.00	164.34	0.00	602.58	90%	60.26
Cintas magneticas información de backups	0.00	54.78	54.78	54.78	54.78	0.00	164.34	0.00	16.43	41.09	164.34	0.00	605.32	90%	60.53
Unidades de Cd. DVD's, Memorias Extraibles	0.00	10.96	10.96	10.96	10.96	0.00	32.87	0.00	0.00	32.87	32.87	0.00	142.43	90%	14.24
															18756.71

Tabla 12: Calculo del Riesgo Residual

Fase 4: Propuesta de Proyectos

El objetivo de la presente fase es detallar los proyectos a realizar para la implementación de las salvaguardas identificadas en el análisis de riesgos realizado en la fase anterior, basados en el objetivo establecido de los controles de la norma que no alcanzaron a cumplirse al 90% según la valoración realizada en el análisis diferencial de la norma ISO 27001 e ISO 27002 versus el estado actual de la organización.

El análisis diferencial arrojo como resultado que los numerales siguientes estaban debajo del 90% de cumplimiento y es donde enfocaremos nuestros proyectos para conseguir que se cumpla el porcentaje buscado

- Numeral 7. Gestión de Activos
- Numeral 8. Seguridad Ligada a los Recursos Humanos
- Numeral 10. Gestión de Comunicaciones y Operaciones
- Numeral 11. Control de Acceso
- Numeral 12. Adquisición, desarrollo y mantenimiento de sistemas de información
- Numeral 13. Gestión de Incidentes de Seguridad

Hay un componente muy importante revisando el detalle del análisis diferencial (Cuadro 1) y es que algunos de los puntos que no alcanzaron el cumplimiento solicitado del 90% tienen como causa la falta de documentación de algunos de los procesos como en los numerales 7, 8, 10, 12 y 13, y en el numeral 11 observamos basados en el análisis de las contramedidas propuestas de la tabla 11, que la mayoría de los proyectos implican implementaciones de soluciones de tecnología.

Los proyectos más significativos son los siguientes:

- Implementación de una solución de SIEM
- Implementación de una solución de integridad de archivos
- Implementación de una solución de inventarios de hardware y software
- Implementación de un segundo firewall para el perímetro interno
- Implementación de una solución de gestión de Vulnerabilidades
- Implementación de una solución de NAC (Network Access Control)
- Implementación de una solución de DLP (Data Loss Prevention)

Para cada uno de estos proyectos se deben cumplir básicamente los siguientes pasos:

- Investigación y selección de soluciones y/o herramientas

  En este punto el personal del área de tecnología y en particular del área de seguridad informática se deben encargar de buscar soluciones y/o herramientas cuyas funciones cumplan con el propósito identificado, para ello se utilizan los reportes de Gartner o sitios web de evaluación de productos como guias y luego de identificar mínimo tres candidatos, se analizan en detalle y se generan cuadros comparativos con las principales características, incluyendo el valor comercial de las mismas
- Pruebas de concepto de las soluciones y/o herramientas

  La realización de pruebas de concepto con las soluciones, implica de las soluciones y/o herramientas previamente identificadas, se contacta con los proveedores (dos o tres) y se solicita una prueba de concepto de la herramienta con el fin de evaluar de manera práctica su funcionalidad, apoyados en estas pruebas se termina el cuadro comparativo de las soluciones y se selecciona el producto /o herramienta más adecuado para cubrir la necesidad identificada.
- Elección de solucion y/o herramienta

  Basados en la tabla comparativa de solución y/o herramientas la dirección de infraestructura selecciona la herramienta más adecuada basados en la relación costo / beneficio, genera una solicitud de compra de la misma (en donde quede la evaluación de los productos, y un concepto técnico que genera una recomendación para elegir una de las herramientas y/o soluciones) la presentación en primera instancia se le envía al gerente del área justificando la necesidad de la misma.
- Proceso de Compra

  Si la presentación tiene el respaldo de la gerencia, se sube al sistema de ERP en donde cursa los niveles de aprobación necesarios (incluyendo la vicepresidencia si la inversión es considerable) para que el departamento de compras finalmente emita correo con la solicitud de compra final al proveedor
- Implementación de la Solución y/o producto comprado

  Una vez el producto y/o solución se compra, se formaliza con el proveedor un plan de trabajo para llevar a cabo la implementación del mismo, con el plan de trabajo se separan los recursos necesarios para acompañar al proveedor en la

implementación y en cualquier caso se debe exigir unas actas de seguimiento del cronograma planteado

- Estabilización de la Solución

  Luego de la fase de implementación sigue una fase de estabilización de la solución y/o producto, en donde se hace seguimiento junto con el proveedor del comportamiento del mismo y se hacen los ajustes necesarios para que su funcionamiento sea lo esperado por la organización, para el caso de los proyectos de tecnología además de esta fase se debe incluir los procesos propios de administración y monitoreo de la solución.

De este análisis podemos concluir que las propuestas de los proyectos son básicamente de dos tipos, los proyectos que implican documentar o revisar que la documentación existente se encuentre debidamente actualizada y los proyectos en los cuales necesitamos realizar implementación de soluciones de tecnología, estos últimos los podemos considerar proyectos transversales a la organización, dado que las soluciones que se implementan le dan nuevos servicios o protegen los servicios existentes para todos los colaboradores de la organización.

Para este tipo de proyectos transversales a toda la organización se requerirán evaluación de diferentes tecnologías, selección de una de las soluciones, procesos de compra y planes de trabajo en conjunto con el proveedor seleccionado para poder realizar la instalación, con los controles de cambios necesarios con el fin de identificar claramente las actividades, los responsables y los tiempos estimados de implementación con el fin de reducir el riesgo de impactar la disponibilidad de alguna de las plataformas que ya se encuentran en operación, de cronograma con las actividades macro se encuentra a continuación

4.1 Proyecto de Revisión y Actualización de Documentación del SGSI

Los puntos en donde debemos realizar, mejorar o actualizar la documentación son básicamente los siguientes:

- Centralizar y consolidar la información de inventarios de hardware y software

- Uso aceptable de activos
- Funciones y Responsabilidades del personal
- Procesos disciplinarios

Para este tipos de proyectos en donde se debe revisar y actualizar la documentación se necesita una participación activa de cada una de las áreas que tiene a cargo la documentación a actualizar y del área de procesos quien encargará a uno o varios de sus analistas para realizar el acompañamiento al área con el fin de generar un documento que cumpla con los lineamientos corporativos y que sea fácil de entender para las personas con el conocimiento específico del área en cuestión.

La documentación generada y/o actualizada deberá ser custodiara por el área y almacenada en la carpeta compartida en donde se encuentran los documentos de los procesos, dicha carpeta será de lectura para los miembros de la organización que en relación a su cargo deban tener acceso a los mismos.

Los documentos deberán ser actualizados al menos una vez al año, con el fin de garantizar que los cambios propios de la madurez de los procesos al interior de la organización se vean reflejados en los mismos, el director y/o gerente del área avalara su actualización por medio de un formato que se llenara y se firmara con la solicitud de publicación de la nueva versión del documento, con el fin de poder realizar seguimiento a las actualizaciones de los mismos y evidenciar la evolución del SGSI.

4.2 Proyectos del SGSI Transversales a la organización

Para los proyectos de corte tecnológico que son transversales a la organización, además de tener que surtir los procesos definidos anteriormente de evaluación, selección y negociación, en la fase de implementación se debe tener especial cuidado y contemplar dentro del detalle de la implementación el rollback de las actividades a realizar, debido a que los elementos de tecnología se encuentran en producción es de vital importancia realizar la planificación necesaria con el fin de no afectar la disponibilidad de los activos de información que se puedan ver impactados por los nuevos ajustes necesarios en el proceso de implementación de las nuevas soluciones

Para la fase de implementación del IDS se deben elegir con cuidado los segmentos de red a proteger, un sistema de detección y prevención de intrusos hace más sentido sobre el segmento de red de la DMZ que sobre un segmento de red interna, así mismo la selección de las alertas configuradas deben corresponder con los activos a proteger con el fin de facilitar el trabajo de la solución, además de la implementación de la herramienta debemos garantizar que exista un claro responsable de las funciones de monitoreo de la solución.

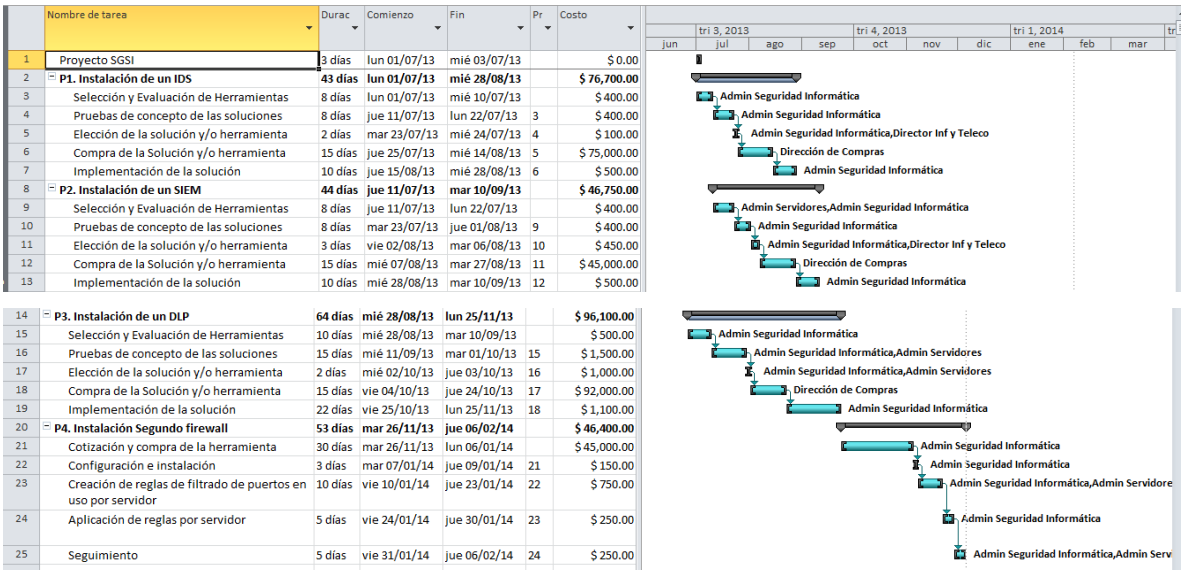
Para la fase de implementación de una solución de SIEM es muy importante contar con el dimensionamiento correcto del espacio necesario para el almacenamiento de datos, los permisos de red necesarios para que le lleguen las alerta de los sistemas a los cuales les centraliza los logs y unos procedimientos de monitoreo adecuados.

Para la fase de implementación de una solución de DLP, la construcción de las cadenas de string a evaluar son de vital importancia para el éxito del proyecto, el control de la fuga de información por medio de la web debe ser un componente que se evalué desde el momento de revisar las soluciones disponibles en el mercado, el proceso de monitoreo debe ser tan bien bastante claro

Para la fase de implementación de un segundo Firewall, debemos iniciar en modo de monitoreo pero sin negar ninguna conexión y luego de revisar los logs resultantes se deben ajustar las reglas para los servidores internos de ser posible basados en los roles de los mismos y de la manera más puntual posible con el fin de no realizar afectación sobre la plataforma

Las anteriores fueron las consideraciones puntuales para las fases de implementación de los proyectos más significativos.

A continuación, se detallan los proyectos transversales de la organización, expresados mediante un diagrama de Gantt, y se anexará a la documentación solicitada



	Nombre de tarea	Durac	Comienzo	Fin	Pr	Costo
1	Proyecto SGSI	3 días	lun 01/07/13	mié 03/07/13		$ 0.00
2	**P1. Instalación de un IDS**	**43 días**	**lun 01/07/13**	**mié 28/08/13**		**$ 76,700.00**
3	Selección y Evaluación de Herramientas	8 días	lun 01/07/13	mié 10/07/13		$ 400.00
4	Pruebas de concepto de las soluciones	8 días	jue 11/07/13	lun 22/07/13	3	$ 400.00
5	Elección de la solución y/o herramienta	2 días	mar 23/07/13	mié 24/07/13	4	$ 100.00
6	Compra de la Solución y/o herramienta	15 días	jue 25/07/13	mié 14/08/13	5	$ 75,000.00
7	Implementación de la solución	10 días	jue 15/08/13	mié 28/08/13	6	$ 500.00
8	**P2. Instalación de un SIEM**	**44 días**	**jue 11/07/13**	**mar 10/09/13**		**$ 46,750.00**
9	Selección y Evaluación de Herramientas	8 días	jue 11/07/13	lun 22/07/13		$ 400.00
10	Pruebas de concepto de las soluciones	8 días	mar 23/07/13	jue 01/08/13	9	$ 400.00
11	Elección de la solución y/o herramienta	3 días	vie 02/08/13	mar 06/08/13	10	$ 450.00
12	Compra de la Solución y/o herramienta	15 días	mié 07/08/13	mar 27/08/13	11	$ 45,000.00
13	Implementación de la solución	10 días	mié 28/08/13	mar 10/09/13	12	$ 500.00
14	**P3. Instalación de un DLP**	**64 días**	**mié 28/08/13**	**lun 25/11/13**		**$ 96,100.00**
15	Selección y Evaluación de Herramientas	10 días	mié 28/08/13	mar 10/09/13		$ 500.00
16	Pruebas de concepto de las soluciones	15 días	mié 11/09/13	mar 01/10/13	15	$ 1,500.00
17	Elección de la solución y/o herramienta	2 días	mié 02/10/13	jue 03/10/13	16	$ 1,000.00
18	Compra de la Solución y/o herramienta	15 días	vie 04/10/13	jue 24/10/13	17	$ 92,000.00
19	Implementación de la solución	22 días	vie 25/10/13	lun 25/11/13	18	$ 1,100.00
20	**P4. Instalación Segundo firewall**	**53 días**	**mar 26/11/13**	**jue 06/02/14**		**$ 46,400.00**
21	Cotización y compra de la herramienta	30 días	mar 26/11/13	lun 06/01/14		$ 45,000.00
22	Configuración e instalación	3 días	mar 07/01/14	jue 09/01/14	21	$ 150.00
23	Creación de reglas de filtrado de puertos en uso por servidor	10 días	vie 10/01/14	jue 23/01/14	22	$ 750.00
24	Aplicación de reglas por servidor	5 días	vie 24/01/14	jue 30/01/14	23	$ 250.00
25	Seguimiento	5 días	vie 31/01/14	jue 06/02/14	24	$ 250.00

Grafica 5: Proyectos a realizar implementación SGSI

Fase 5: Auditoria de Cumplimiento

5.1 Metodología

Para el desarrollo de la fase cinco (5) en donde se ejecutara la auditoria de cumplimiento, se usará el modelo de madurez de la capacidad (CMM) como metodología para el análisis del grado de madurez en la implementación del SGSI (Sistema de Gestión De Seguridad de la Información) en la implementación de la norma ISO 27001:2007, que agrupa un total de 133 controles sobre las recomendaciones de buenas prácticas para la Gestión de la Seguridad de la Información que está organizado en 11 áreas y que cuenta con 39 objetivos de control, así como los controles descriptos en la norma ISO/IEC 27002:2009

Como base de Conocimiento para el análisis se tomaran las valoraciones siguientes:

Efectividad	CMM	Significado	Descripción
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible No se ha reconocido siquiera que existe un problema a resolver
10%	L1	Inicial /Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoria de veces en el esfuerzo personal Los procesos son inexistentes o localizadaos en áreas concretas. No existen plantillas definidas a nivel corporativo
50%	L2	Repetible pero Intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al metodo No hay comunicación o entrenamiento Formal, las responsabilidades quedan a cargo de cada individuo Se depende del grado de conocimiento de cada individuo
90%	L3	Proceso Definido	La organización entera participa en el proceso Los procesos estan implantados, documentados y comunicados mediante entrenamiento
95%	L4	Gestionado y Medible	Se puede seguir con indicadores números y estadisticos la evolución de los procesos Se dispone de tecnología para automaticar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia
100%	L5	Optimizado	Los procesos están bajo constante mejora En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos

Tabla 13: Valoraciones criterios de Madurez CMM

5.2 Evaluación de la Madurez

El objetivo de esta fase es evaluar el nivel de madurez implementado en la seguridad en lo que respecta a los diferentes dominios de control y los 133 controles planteados por la norma ISO 27001:2007, y los controles descriptivos en la norma ISO 27002:2009

La presente evaluación se ejecutó tomando como fuentes de información principales y evidencia los siguientes documentos y el estado actual de la implementación de la norma ISO 27001 e ISO 27002 en la organización

- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Control de Acceso
- Cumplimiento
- Gestión de Activos
- Gestión de Comunicaciones y Operaciones
- Gestión de Continuidad del Negocio
- Gestión de Incidentes
- Organización de la Seguridad de la Información
- Política de Personal
- Política de Seguridad de la Información
- Seguridad Física y Ambiental
- Seguridad en los Recursos Humanos

Con esta información y realizando énfasis en los objetivos de control que se identificaron inicialmente como incumplidos por estar por debajo del 90%, se realizó la auditoria y se encontraron los siguientes resultados

Evaluación de la Madurez

Amenaza	Activo	Impacto Potencial	Salvaguarda	Objetivos de Contol ISO 27002	Madurez CMM%
Hurto de Codigo Fuente	Servidor HP NonStop	9	Se restrigiran las cuentas de usuario con rol de administrador	11.1.1 Politica de Control de Acceso	90%
	Servidor AS/400	9	Se ejecutaran auditorias de control y seguimiento	11.2.2 Gestion de Privilegios	90%
	Servidor EFT	9	Se realizaran las aoperaciones basados en las mejores practicas	5.1.1 Documento de politica de Seguridad de la Información	95%
	Servidor E-commerce	9		10.7.2 Retirada de Soportes	85%
	Servidor E-commerce	9		10.7.3 Procedimientos de manipulación de la Información	90%
	Codigo Fuente de Programas	10		7.1.3 Uso aceptable de activos	90%
	Discos Duros Servidores y estaciones de trabajo	9			
	Cintas magneticas información de backups	9			
	Unidades de Cd. DVD's, Memorias Extraibles	9			
Hurto de Hardware	Servidor HP NonStop	10	Se estableceran procedimientos para el ingreso y retiro de equipos y partes	9.1.1 Perimetro de Seguridad Fisica	95%
	Servidor AS/400	10	Se estableceran procedimientos para el uso de medios extraibles	9.1.4 Protección contras las amenazas externas y de origen ambiental	90%
	Servidor EFT	9	Se estableceran procedimientos para la asignación de equipos a los usuarios	9.2.1 Emplazamiento y protección de equipos	90%
	Servidor E-commerce Web	9		9.2.2 Instalaciones de suministro	90%
	Servidor E-commerce DB	9		9.2.6 Reutilización o retirada segura de equipos	90%
	Servidor ERP	9		9.2.7 Retirada de materiales propiedad de la empresa	95%
	Servidor Nomina	9		10.7.1 Gestion de soportes extraibles	95%
	Servidor Directorio Activo	9		10.7.2 Retirada de Soportes	95%
	Servidor de Correo electrónico	8			
	Servidor Antivirus	6			
	Servidor de Backups	8			
	Equipos Escritorio, Portatiles, SmarthPhones	6			
	Equipos de Teleco: Cisco Catalys 7200	9			
	Equipos de Seg Perimetral: Firewall Cisco ASA	9			
	Equipos de Seg Perimetral: Appliance de IDS e IPS	9			
	Central Telefonica: Alcatel 5500	8			
	Equipos POS	9			
	Discos Duros Servidores y estaciones de trabajo	10			
	Cintas magneticas información de backups	8			
	Unidades de Cd. DVD's, Memorias Extraibles	9			
Inundación	CPD: Centro de Computo Principal	10	Se estableceran y probaran planes de contingencia	9.1.4 Protección contra las amenazas externas y de origen ambiental	90%
	Dirección de Infraestructura y Telecomunicaciones	8	Se estableceran procedimientos de protección de equipos	9.2.1 Emplazamiento y protección de equipos	95%
	Sala Electrica, UPS y Plantas de Energia	10	Se estableceran y probaran planes de evacuación	9.1.3 Seguridad de oficinas, despachos e instalaciones	95%
	Servidor HP NonStop	10	Se estableceran planes de recuperación de desastres	9.2.2 Instalaciones de Suministro	90%
	Servidor AS/400	10			
	Servidor EFT	10			
	Servidor E-commerce Web	10			
	Servidor E-commerce DB	10			
	Servidor ERP	9			
	Servidor Nomina	9			
	Servidor Directorio Activo	8			
	Servidor de Correo electrónico	8			
	Servidor Antivirus	6			
	Servidor de Backups	8			
	Equipos Escritorio, Portatiles, SmarthPhones	9			
	Equipos de Telecomunicaciones: Cisco Catalys 7200	10			
	Equipos de Seguridad Perimetral: Firewall Cisco ASA	10			
	Equipo de Seguridad Perimetral: Appliance de IDS e IPS	10			
	Central Telefonica: Alcatel 5500	9			
	Equipos POS	10			
	Sistemas de Alimentación Interrumpida (UPS)	10			
	Sistemas generadores de Energia	10			
	Sistemas de aire acondicionado Ambiental y de Precision	10			
	Sistema de Cableado Electrico	8			
	Director de Infraestructura y Telecomunicaciones	10			
	Administradores (Seg, SO, Bases de Datos)	10			
	Desarrolladores	10			
	Director de Sistemas 1 (Diseño y Desarrollo)	10			
	Proveedores	10			
	Discos Duros Servidores y estaciones de trabajo	10			
	Cintas magneticas información de backups	10			
	Unidades de Cd. DVD's, Memorias Extraibles	10			
Terremoto	CPD: Centro de Computo Principal	8	Se estableceran y probaran planes de contingencia	9.1.3 Seguridad de oficinas, despachos e instalaciones	95%
	Dirección de Infraestructura y Telecomunicaciones	8	Se estableceran procedimientos de protección de equipos	9.1.4 Protección contra las amenazas externas y de origen ambiental	90%
	Sala Electrica, UPS y Plantas de Energia	8	Se estableceran y probaran planes de evacuación	9.1.5 Trabajo en áreas seguras	90%
	Servidor HP NonStop	7	Se estableceran planes de recuperación de desastres	10.1.2 Continuidad del Negocio y evaluación de riesgos	85%
	Servidor AS/400	7			
	Servidor EFT	7			
	Servidor E-commerce Web	7			
	Servidor E-commerce DB	7			
	Servidor ERP	7			
	Servidor Nomina	7			
	Servidor Directorio Activo	7			
	Servidor de Correo electrónico	7			
	Servidor Antivirus	6			
	Servidor de Backups	7			
	Equipos Escritorio, Portatiles, SmarthPhones	6			
	Equipos de Telecomunicaciones: Cisco Catalys 7200	6			
	Equipos de Seguridad Perimetral: Firewall Cisco ASA	6			
	Equipo de Seguridad Perimetral: Appliance de IDS e IPS	6			
	Central Telefonica: Alcatel 5500	6			
	Equipos POS	6			
	Red de Datos:Ethernet	7			
	Red de Telefonia: Ethernet (Voz IP)	7			
	Acceso a Internet: Fibra Optica	7			
	Sistemas de Alimentación Interrumpida (UPS)	7			
	Sistemas generadores de Energia	7			
	Sistemas de aire acondicionado Ambiental y de Precision	7			
	Sistema de Cableado Electrico	7			
	Director de Infraestructura y Telecomunicaciones	8			
	Administradores (Seg, SO, Bases de Datos)	8			
	Desarrolladores	8			
	Director de Sistemas 1 (Diseño y Desarrollo)	8			
	Proveedores	8			
	Discos Duros Servidores y estaciones de trabajo	7			
	Cintas magneticas información de backups	7			
	Unidades de Cd. DVD's, Memorias Extraibles	7			

Evaluación de la Madurez

Amenaza	Activo	Impacto Potencial	Salvaguarda	Objetivos de Contol ISO 27002	Madurez CMM%
Incendio	CPD: Centro de Computo Principal	9	Se estableceran y probaran planes de contingencia	9.1.3 Seguridad de oficinas, despachos e instalaciones	95%
	Dirección de Infraestructura y Telecomunicaciones	9	Se estableceran procedimientos de protección de equipos	9.1.4 Protección contra las amenazas externas y de origen ambiental	90%
	Sala Electrica, UPS y Plantas de Energia	9	Se estableceran y probaran planes de evacuación	9.1.5 Trabajo en áreas seguras	90%
	Servidor HP NonStop	9	Se estableceran planes de recuperación de desastres	10.1.2 Continuidad del Negocio y evaluación de riesgos	85%
	Servidor AS/400	9			
	Servidor EFT	9			
	Servidor E-commerce Web	9			
	Servidor E-commerce DB	9			
	Servidor ERP	9			
	Servidor Nomina	9			
	Servidor Directorio Activo	9			
	Servidor de Correo electrónico	9			
	Servidor Antivirus	8			
	Servidor de Backups	9			
	Equipos Escritorio, Portatiles, SmarthPhones	9			
	Equipos de Telecomunicaciones: Cisco Catalys 7200	9			
	Equipos de Seguridad Perimetral: Firewall Cisco ASA	9			
	Equipo de Seguridad Perimetral: Appliance de IDS e IPS	9			
	Central Telefonica: Alcatel 5500	9			
	Equipos POS	9			
	Red de Datos:Ethernet	9			
	Red de Telefonia: Ethernet (Voz IP)	9			
	Acceso a Internet: Fibra Optica	9			
	Sistemas de Alimentación Interrumpida (UPS)	9			
	Sistemas generadores de Energia	9			
	Sistemas de aire acondicionado Ambiental y de Precision	9			
	Sistema de Cableado Electrico	9			
	Director de Infraestructura y Telecomunicaciones	9			
	Administradores (Seg, SO, Bases de Datos)	9			
	Desarrolladores	9			
	Director de Sistemas 1 (Diseño y Desarrollo)	9			
	Proveedores	9			
	Discos Duros Servidores y estaciones de trabajo	9			
	Cintas magneticas información de backups	9			
	Unidades de Cd. DVD's, Memorias Extraibles	9			
Ejecución Software Malicioso	SO. HP NonStop	10	Se implementara un IDS y un Firewall para detectar trafico de red malicioso	10.4.1 Controles contra software malicioso	95%
	AIX version 7.1	10	Se desarrollara un plan de continuidad del negocio	10.4.2 Controles contra el código descargado en el cliente	95%
	OS/400 7.1	10	Se reslizara una evaluación de riesgos de manera periodica	11.4.1 Politicas de uso de los servicios de red	90%
	Sistema Operativo: Windows Server 2012	9	Se implementara un sistema de AntiSpam para controlar los correos no deseados	14.1.2 Continuidad del negocio y evaluación de riesgos	85%
	Sistema Operativo: Windows 7 Profesional	9		14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad	90%
	Bases de Datos: Oracle 11G	10			
	Correo Electronico: Lotus Notes 8.5	9			
	Antivirus: Symantec	7			
	WebServer: Iplanet	9			
	Sistema de Backups: Symantec Backup Exec	10			
	IPS e IDS: Palo Alto Network	10			
	Discos Duros Servidores y estaciones de trabajo	8			
	Cintas magneticas información de backups	8			
	Unidades de Cd. DVD's, Memorias Extraibles	8			
	Codigo Fuente de Programas	10			
Acceso Fisico no Autorizado	CPD: Centro de Computo Principal	9	Se implementara un sistema de control de ingreso con biometria y/o tarjeta magnetica	9.2.1 Emplazamiento y protección de equipos	95%
	Dirección de Infraestructura y Telecomunicaciones	8	Se establecera un proceso estricto de control de ingreso al CPD	9.1.2 Conroles fisicos de entrada	95%
	Sala Electrica, UPS y Plantas de Energia	8	Se establecera un sistema de control por CCVT en las áreas sensibles	9.2.1 Emplazamiento y protección de equipos	90%
	Servidor HP NonStop	9	Se estableceran procedimiento de ingreso a cuartos electricos, UPS's y Plantas Electricas	9.1.2 Controles fisicos de entrada	95%
	Servidor AS/400	9		11.1.1 Politica de control de acceso	90%
	Servidor EFT	9		11.2.2 Gestion de privilegios	90%
	Servidor E-commerce Web	9		11.4.1 Politica de uso de los servicios en red	90%
	Servidor E-commerce DB	9		11.5.4 Uso de los recursos del sistema	90%
	Servidor ERP	9			
	Servidor Nomina	9			
	Servidor Directorio Activo	9			
	Servidor de Correo electrónico	9			
	Servidor Antivirus	9			
	Servidor de Backups	8			
	Equipos Escritorio, Portatiles, SmarthPhones	9			
	Equipos de Telecomunicaciones: Cisco Catalys 7200	8			
	Equipos de Seguridad Perimetral: Firewall Cisco ASA	8			
	Equipo de Seguridad Perimetral: Appliance de IDS e IPS	8			
	Central Telefonica: Alcatel 5500	9			
	Equipos POS	10			
	Red de Datos:Ethernet	10			
	Red de Telefonia: Ethernet (Voz IP)	10			
	Acceso a Internet: Fibra Optica	10			
	Sistemas de Alimentación Interrumpida (UPS)	9			
	Sistemas generadores de Energia	9			
	Sistemas de aire acondicionado Ambiental y de Precision	9			
	Sistema de Cableado Electrico	9			
	Discos Duros Servidores y estaciones de trabajo	9			
	Cintas magneticas información de backups	9			
	Unidades de Cd. DVD's, Memorias Extraibles	9			
Acceso logico no Autorizado	SO. HP NonStop	10	Se implementara un sistema de detección de Intrusos	9.2.1 Emplazamiento y protección de equipos	95%
	AIX version 7.1	10	Se implementara un segundo firewall para los segmentos de Servidores criticos	9.1.2 Controles fisicos de entrada	95%
	OS/400 7.1	10	Se implementara una solución de NAC (Network Access Control)	11.1.1 Politica de Control de acceso	90%
	Sistema Operativo: Windows Server 2012	9	Se implementara una solución de centralización y correlación de eventos (SIEM)	11.2.2 Gestion de Privilegios	90%
	Sistema Operativo: Windows 7 Profesional	9	Se estableceran estrictos procedimientos de control de acceso logico	11.2.3 Gestion de Contraseñas de usuario	95%
	Bases de Datos: Oracle 11G	10	Se implementaran solución de monitoreo de integridad de archivos en rutas criticas	11.2.4 Revisión de los derechos de usuarios	90%
	Correo Electronico: Lotus Notes 8.5	9	Se estableceran permisos de acceso administrativos filtrados por el firewall	11.2.1 Registro de usuarios	95%
	Antivirus: Symantec	8		11.4.1 Politica de uso de los servicios en red	90%
	WebServer: Iplanet	9		11.5.4 Uso de los recursos del sistema	90%
	Sistema de Backups: Symantec Backup Exec	9		11.6.1 Restricción del acceso a la información	95%
	IPS e IDS: Palo Alto Network	9		9.1.1 Perimetro de Seguridad Fisica	95%
	Información de Tarjetahabientes	10		11.7.1 Ordenadores Portatiles y comunicaciones moviles	90%
	Codigo Fuente de Programas	10			
	Registros de Actividad: Logs de software base y Aplicaciones	8			
	Red de Datos:Ethernet	10			
	Red de Telefonia: Ethernet (Voz IP)	9			
	Acceso a Internet: Fibra Optica	10			
	Sistemas de Alimentación Interrumpida (UPS)	9			
	Sistemas de aire acondicionado Ambiental y de Precision	9			
	Discos Duros Servidores y estaciones de trabajo	10			
	Cintas magneticas información de backups	8			
	Unidades de Cd. DVD's, Memorias Extraibles	10			

Evaluación de la Madurez					
Amenaza	Activo	Impacto Potencial	Salvaguarda	Objetivos de Contol ISO 27002	Madurez CMM%
Incumplimiento Legal	Servidor HP NonStop	10	Se estableceran SLA con terceros	15.1.1 Identificación de la legislación aplicable	100%
	Servidor AS/400	10	Se implementaran polizas de seguro con cubrimiento por responsabilidad civil	15.1.2 Derechos de propiedad Intelectual	90%
	Equipos POS	10		6.2.2 Tratamiento de la seguridad en la relación con los clientes	95%
Indisponibilidad de Recursos Humanos	Director de Infraestructura y Telecomunicaciones	9	Se estableceran procedimientos de backups en cargos criticos	14.1.2 Continuidad del Negocio y análisis de impacto	90%
	Administradores (Seg, SO, Bases de Datos)	9	Se implementara en el plan de continuidad un apartado para el recurso Humano		
	Desarrolladores	8			
	Director de Sistemas 1 (Diseño y Desarrollo)	9			
	Proveedores	8			
Filtración de datos personales o tecnicos	Información de Tarjetahabientes	10	Se estableceran acuerdos de confidencialidad con expleados y proveedores	9.2.3 Seguridad del cableado	95%
	Codigo Fuente de Programas	10	Se contrataran polizas de seguros para casos de filtración de datos	10.10.2 Supervisión de uso del sistema	90%
	Registros de Actividad: Logs de software base y Aplicaciones	8		11.1.1 Politica de control de acceso	90%
	Red de Datos:Ethernet	10		11.4.5 Segregación de las redes	95%
	Red de Telefonia: Ethernet (Voz IP)	9		11.4.6 Control de la conexión a la red	85%
	Acceso a Internet: Fibra Optica	10		11.5.1 Procedimientos seguros de inicio de sesión	90%
Fallas en las Telecomunicaciones	Red de Datos:Ethernet	10	Se estableceran SLA con proveedores de telecomunicaciones	10.2.1 Provisión de Servicios	90%
	Red de Telefonia: Ethernet (Voz IP)	10	Se contraran canales de backup para los enlaces principales	10.2.2 Supervisión de los servicios prestados por terceros	90%
	Acceso a Internet: Fibra Optica	10	Se estableceran procesos proactivos de monitoreo de los canales	10.2.3 Gestion del cambio en los servicios prestados por terceros	80%

Tabla 14: Evaluación de Madurez

5.3 Presentación de Resultados

El detalle de las áreas que estaban incumplidas al iniciar el proyecto luego de la auditoria es el siguiente:

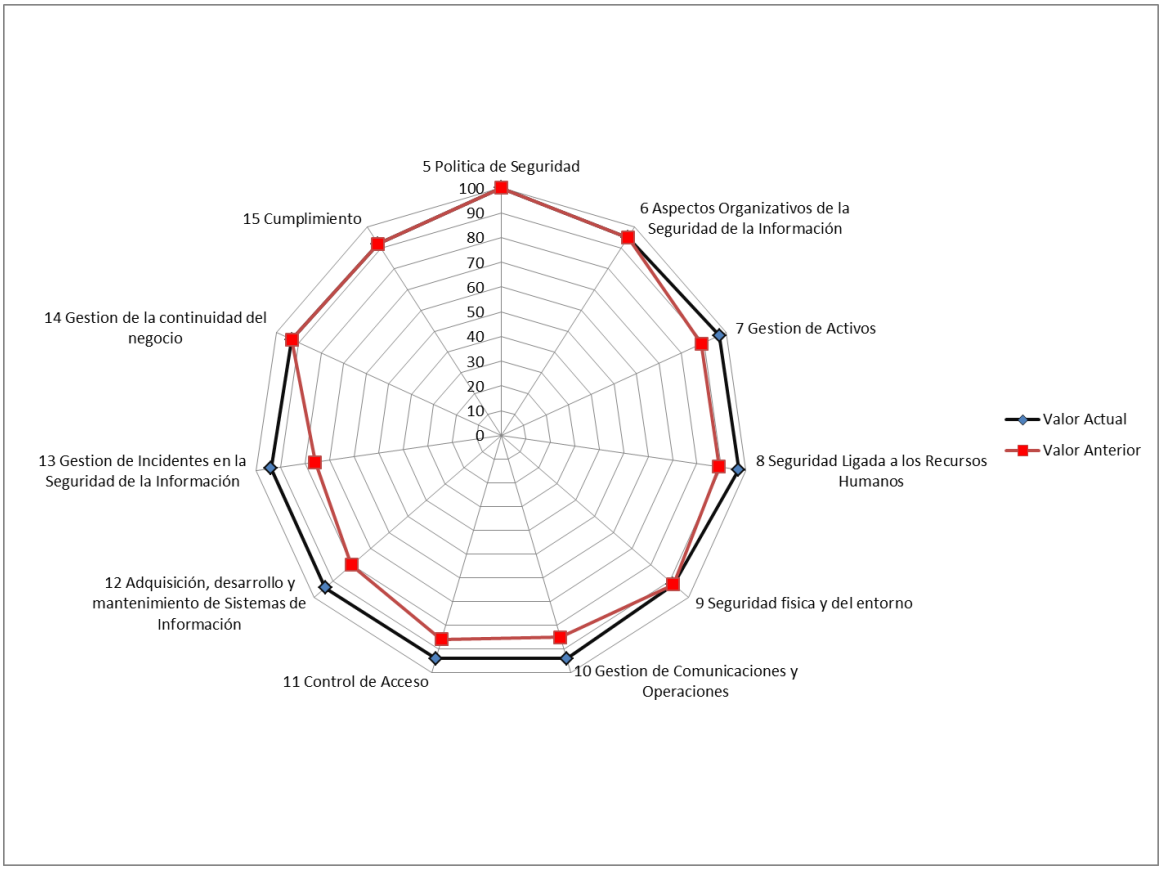
7	GESTION DE ACTIVOS			
	7.1	Responsabilidad sobre los activos		
		7.1.1	Inventario de Activos	95%
		7.1.2	Propiedad de los Activos	100%
		7.1.3	Uso aceptable de los activos	95%
	7.2	Clasificación de la Información		
		7.2.1	Directrices de clasificación	100%
		7.2.2	Etiquetado y Manipulado de la Información	95%
8	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
	8.1	Antes del empleo		
		8.1.1	Funciones y Responsabilidades	95%
		8.1.2	Investigación de Antecedentes	100%
		8.1.3	Terminos y Condiciones de Contratación	100%
	8.2	Durante el empleo		
		8.2.1	Responsabilidades de la Dirección	95%
		8.2.2	Concientización, formación y capacitación en Seguridad de la Información	100%
		8.2.3	Proceso Disciplinario	95%
	8.3	Cese del Empleo o cambio de Puesto de Trabajo		
		8.3.1	Responsabilidad del Cese o Cambio	95%
		8.3.2	Devolución de Activos	95%
		8.3.3	Retirada de los derechos de Acceso	95%
10	GESTION DE COMUNICACIONES Y OPERACIONES			
	10.1	Responsabilidad y procedimientos de Operación		
		10.1.1	Documentación de los procedimientos de Operación	95%
		10.1.2	Gestion de cambios	95%
		10.1.3	Segregación de funciones	95%
		10.1.4	Separación de recursos de desarrollo, prueba y operación	90%
	10.2	Gestion de la Prestación del servicio por terceros		
		10.2.1	Prestación del Servicio	90%
		10.2.2	Monitoreo y revisión de los servicios prestados por terceros	90%
		10.2.3	Gestion del cambio en los servicios prestados por terceros	95%

	10.3	Planificación y aceptación del sistema		
		10.3.1	Gestion de la capacidad	90%
		10.3.2	Aceptación del Sistema	90%
	10.4	Protección contra el codigo malicioso y descargable		
		10.4.1	Controles contra el codigo malicioso	100%
		10.4.2	Controles contra el codigo descargado en el cliente	100%
	10.5	Copias de Seguridad		
		10.5.1	Copias de seguridad de la información	95%
	10.6	Gestion de la Seguridad de las Redes		
		10.6.1	Controles de Red	95%
		10.6.2	Seguridad de los Servicios de Red	95%
	10.7	Manipulación de los Soportes		
		10.7.1	Gestion de Soportes Extraibles	95%
		10.7.2	Retirada de soportes	95%
		10.7.3	Procedimiento para el manejo de la información	90%
		10.7.4	Seguridad de la Documentación del Sistema	95%
	10.8	Intercambio de Información		
		10.8.1	Politicas y procedimientos de Intercambio de Información	95%
		10.8.2	Acuerdos de Intercambio	90%
		10.8.3	Soportes fisicos en transito	95%
		10.8.4	Mensajeria electronica	95%
		10.8.5	Sistemas de información empresariales	90%
	10.9	Servicios de comercio electrónico		
		10.9.1	Comercio Electrónico	95%
		10.9.2	Transacciones en Linea	90%
		10.9.3	Información Publicamente Disponible	90%
	10.10	Monitoreo		
		10.10.1	Registros de Auditoria	90%
		10.10.2	Monitoreo del uso del sistema	95%
		10.10.3	Protección de la información de los registros	95%
		10.10.4	Registros de administración y operación	95%
		10.10.5	Registro de Fallos	95%
		10.10.6	Sincronización del Reloj	95%
11	CONTROL DE ACCESO			
	11.1	Requisitos de negocio para el control de acceso		
		11.1.1	Politica de control de acceso	90%
	11.2	Gestion de acceso de usuario		
		11.2.1	Registro de Usuarios	95%
		11.2.2	Gestion de Privilegios	95%
		11.2.3	Gestion de Contraseñas de Usuario	95%
		11.2.4	Revisión de los derechos de acceso de usuario	90%
	11.3	Responsabilidades de Usuario		
		11.3.1	Uso de contraseñas	95%
		11.3.2	Equipo de usuario desantendido	95%
		11.3.3	Politica de puesto de trabajo Despejado y pantalla limpia	95%
	11.4	Control de Acceso a la red		
		11.4.1	Politica de uso de los servicios en red	95%
		11.4.2	Autenticación de usuario para conexiones externas	90%
		11.4.3	Identificación de los equipos en las redes	95%
		11.4.4	Protección de los puertos de diagnostico y configuración remotos	95%
		11.4.5	Segregación de las redes	95%
		11.4.6	Control de la conexión a la red	95%
		11.4.7	Control de encaminamiento (routing) de red	95%

	11.5	Control de acceso al sistema Operativo		
		11.5.1	Procedimientos seguros de inicio de sesión	95%
		11.5.2	Identificación y autenticación de usuario	95%
		11.5.3	Sistema de gestion de contraseñas	90%
		11.5.4	Uso de los recursos del sistema	90%
		11.5.5	Desconexión automática de sesión	95%
		11.5.6	Limitación del tiempo de conexión	95%
	11.6	Control de acceso a las aplicaciones y a la Información		
		11.6.1	Restricción del acceso a la información	95%
		11.6.2	Aislamiento de sistemas sensibles	95%
	11.7	Ordenadores portátiles y teletrabajo		
		11.7.1	Ordenadores portátiles y comunicaciones móviles	95%
		11.7.2	Teletrabajo	90%
12	ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
	12.1	Requisitos de Seguridad de los sistemas de información		
		12.1.1	Analisis y especificación de los requisitos de Seguridad	95%
	12.2	Tratamiento correcto de las aplicaciones		
		12.2.1	Validación de los datos de entrada	95%
		12.2.2	Control de procesamiento Interno	95%
		12.2.3	Integridad de los mensajes	90%
		12.2.4	Validación de los datos de salida	95%
	12.3	Controles Criptograficos		
		12.3.1	Politica sobre el uso de uso de controles criptograficos	90%
		12.3.2	Gestion de claves	95%
	12.4	Seguridad de los archivos de sistema		
		12.4.1	Control del software operativo	95%
		12.4.2	Protección de los datos de pruebas del sistema	90%
		12.4.3	Control de acceso al código fuenre de los programas	95%
	12.5	Seguridad en los procesis de desarrollo y soporte		
		12.5.1	Procedimientos de control de cambios	95%
		12.5.2	Revisión Técnica de las aplicaciones tras efectuar cambios en el S.O.	95%
		12.5.3	Restricciones a los cambios en los paquetes de software	95%
		12.5.4	Fugas de Información	90%
		12.5.5	Desarrollo del software contratato externamente	95%
	12.6	Gestión de la vulnerabilidad técnica		
		12.6.1	Control de las vulnerabilidades tecnicas	95%
13	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN			
	13.1	Notificación de Eventos y puntos debiles de seguridad de la Información		
		13.1.1	Reporte sobre los eventos de seguridad de la Información	95%
		13.1.2	Reporte sobre las debilidades en la seguridad	95%
	13.2	Gestión de Incidentes y mejoras de seguridad de la Información		
		13.2.1	Responsabilidades y Procedimientos	95%
		13.2.2	Aprendizaje de los incidentes de seguridad de la Información	90%
		13.2.3	Recopilación de evidencias	95%

Tabla 15: Madurez controles ISO 27002

La presentación de los resultados luego de la auditoria versus los obtenidos al inicio de la implementación del SGSI para los objetivos de control que estaban por debajo del 90%, se observa en la siguiente gráfica, en donde el avance es evidente



Grafica 5: Diagrama comparativo evolución estado de madurez controles ISO 27002

BIBLIOGRAFÍA

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184

Recuperada Marzo 2013

- Magerit - Version 3 - Libro I Método
- Magerit - Versión 3 - Libro II Catálogo de Elementos
- Magerit - Versión 3 - Libro III Guía de Técnicas

http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

NIST Guide for Conducting Risk Assessments

Recuperada Marzo 2013

http://www.iso27002.es/

Portal de Soluciones técnicas y organizativas a los controles de la Norma Internacional ISO/IEC 27002

Recuperada Marzo 2013

Glosario de Términos

Activos Informáticos: Son los bienes de la organización que se encuentran relacionados de manera directa o indirecta con la actividad informática, como los servicios, las aplicaciones o software de los equipos informáticos, equipamiento auxiliar, redes de comunicaciones e instalaciones que las soportan.

Antivirus: Software diseñado para prevenir, detectar y eliminar malware (software dañino) de varias categorías

Autenticidad y no repudio: Característica que garantiza que la identidad de los usuarios o procesos que tratan la información y de la autoría de una determinada acción

Backup o copia de Seguridad: Hace referencia a los procesos de copia de la información a medios de almacenamiento como medidas de precaución que facilitan su recuperación en caso de incidentes, con el fin de soportar o respaldar la información de los procesos críticos de la organización

Confidencialidad: Propiedad de la información que garantiza que la misma solo es accedida por las personas que cuentan autorización para ello.

Firewall: Cortafuegos o Firewall es un software que se implementa con el fin de hacer segregación de redes a nivel de comunicaciones, para permitir o denegar los accesos basados en conjuntos de reglas desde y hacia los sistemas que esta protegiendo

IDS/IPS: Intrusion Detection System / Intrusion Prevention System, sistema de prevención y/o detección de intrusos, es un sistema que revisa el tráfico en busca de patrones que coincidan con firmas de ataques conocidos con el fin de detector acciones maliciosas hacia los sistemas que protege

Integridad: Propiedad de la información que asegura que la información y sus métodos de procesamiento son exactos y completos y que la misma no se puede manipular sin autorización

Privacidad: Propiedad de la información que garantiza que solo las personas debidamente autorizadas, tendrán acceso a la misma con los permisos requeridos

Riesgo Intrínseco: Es el riesgo calculado sin tener en consideración las diferentes medidas de seguridad que ya están implantadas en la organización

Riesgo Residual: Es el riesgo calculado tras la aplicación de las salvaguardas o controles, será un riesgo que la organización deba asumir ante la imposibilidad de proteger los activos al 100%

Salvaguarda o Contramedida: Es la medida o medidas de control que se establecen para evitar una situación de riesgo

Software: Conjunto lógico de instrucciones que los sistemas de cómputo interpretan y/o ejecutan para llevar a cabo determinadas tareas.

Trazabilidad: Propiedad de la información que garantiza el seguimiento en la creación, manipulación o eliminación de la misma de los diferentes medios en donde se crea, almacena y/o transmite