ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL EDCOM

PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE: ANALISTA DE SISTEMAS

TEMA

"IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN APLICADA AL PROCESO DE DESARROLLO DE SOFTWARE A LA MEDIDA PARA LA EMPRESA CORLASOSA"

AUTORES

CLEOFE ASENCIO VERA
JAIME CEBALLOS ARELLANO
JUAN LUNG ALVAREZ

DIRECTOR

MBA. VÍCTOR MUÑOZ CHACHAPOLLA

AÑO
2012

AGRADECIMIENTO

Ante todo, agradecemos a Dios Padre Todopoderoso, porque Él es quien nos provee de Su Sabiduría, inteligencia y talentos para poder realizar de manera diligente y profesional el presente trabajo.

A nuestros padres, quienes desde pequeños nos han guiado a lo largo de nuestra vida estudiantil, nos han apoyado en todo aspecto y siempre han estado a nuestro lado, siendo testigos de nuestra dedicación y esfuerzo diario.

A nuestros profesores, quienes son nuestros segundos padres, y nos entregan sus conocimientos para nuestra correcta formación académica y ética, además de su paciencia para hacer cumplir los objetivos trazados cada semestre, viendo la cátedra que nos imparte.

A la ESPOL, institución que nos acogió durante todos estos años de esfuerzo conjunto, y en donde hemos adquirido las herramientas necesarias para lograr nuestras metas profesionales y académicas.

DEDICATORIA

El presente trabajo lo dedicamos a Dios Padre, como una retribución a Su Sabiduría, dones y talentos que Él en su Soberanía nos ha dado.

A nuestros padres, profesores y compañeros, con quienes hemos compartido grandes momentos, y quienes han estado siempre, cuando hemos requerido de su ayuda.

Especial agradecimiento a nuestro director de tesis, el Máster Víctor H. Muñoz Ch, quien nos ha ayudado con la realización del presente trabajo. A mis compañeros, quienes han dado toda su capacidad y entrega para cumplir con todas las expectativas puestas en la realización del proyecto.

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Trabajo Final de Graduación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral

FIRMAS DEL DIRECTOR DEL PROYECTO Y MIEMBROS DEL TRIBUNAL

MBA. Víctor Hugo Muñoz Chachapolla
Director del Proyecto

MAE. Enrique Salazar Meza
Delegado

FIRMA DE LOS AUTORES DEL PROYECTO DE GRADUACIÓN

CLEOFE ASENCIO VERA

JAIME CEBALLOS ARELLANO

JUAN LUNG ÁLVAREZ

RESUMEN

El presente trabajo se trata de la implementación del Sistema de Seguridad de Gestión de la Información (SGSI) a la empresa CORLASOSA (Corporación Latinoamericana de Software S. A.), basado en la norma ISO 27001.

Mediante la documentación, se pretende demostrar cómo cada una de los activos tangibles e intangibles que posee la Empresa, está expuesta a errores y amenazas, tanto internas como externas, y cómo la implementación del SGSI ayudará a disminuir de manera significativa los riesgos a los que están expuestos.

Para la implementación de la norma, se ha identificado la actividad principal de la Empresa, siendo ésta la del desarrollo de software a la medida. Por ello, se ha determinado que el dominio a seguir es el 12: Adquisición, mantenimiento y desarrollo de software a la medida.

Después del detallado de los activos que intervienen en dicho dominio, se ha recopilado la valoración asignada a los mismos, se las ha tabulado, y con dichos resultados, se ha establecido el respectivo análisis de riesgos.

Luego de ello, se establece, según las mejores prácticas, los controles a seguir, cuyo objetivo es minimizar de manera significativa los riesgos, para que la información permanezca confidencial y accesible a las personas designadas por parte de la empresa.

ÍNDICE GENERAL

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

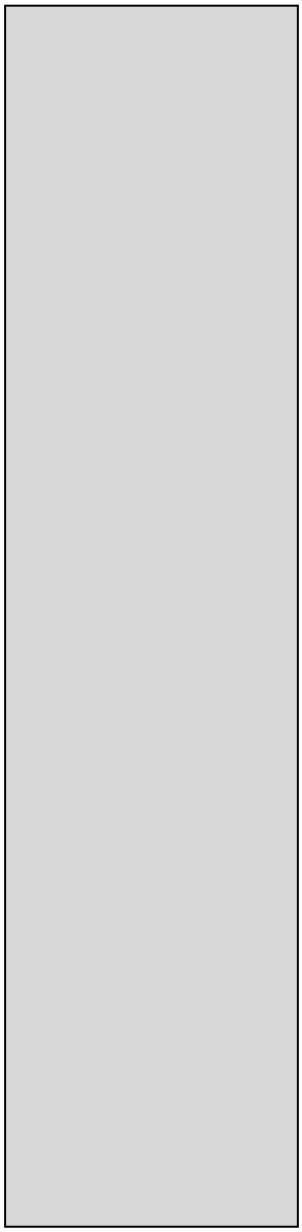
CAPÍTULO 5

CAPÍTULO 6

CAPÍTULO 7

ÍNDICE DE FIGURA

ÍNDICE DE TABLA



CAPÍTULO 1
CONCEPTOS Y NORMAS

1. CONCEPTOS Y NORMAS

1.1. Sistema de Gestión de Seguridad de la Información

La información es el principal activo de muchas organizaciones y necesita ser protegida adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio.

En la actualidad, las empresas de cualquier actividad se enfrentan cada vez más con riesgos e inseguridades tanto internas y externas, las cuales pueden alterar de manera considerable los sistemas de información, la información procesada y almacenada.

Ante tales circunstancias, las organizaciones deben establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio, estableciendo como prioridad la protección de la información.

Para ello, existe la implementación del **Sistema de Gestión de Seguridad de la Información (SGSI).** El SGSI consiste en procesos y controles diseñados para proteger la información de su divulgación no autorizada, transferencia, modificación o destrucción, a los efectos de:

- ✓ **asegurar la continuidad del negocio;**
- ✓ **minimizar posibles daños al negocio;**
- ✓ **maximizar oportunidades de negocios.**

"La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada."

La seguridad de la información se caracteriza aquí como la preservación de:

- su confidencialidad**, asegurando que sólo quienes estén autorizados pueden acceder a la información;**
- su integridad**, asegurando que la información y sus métodos de proceso son exactos y completos.**
- su disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.**

La seguridad total es inalcanzable, pero mediante los procesos de mejora continua del SGSI, se puede conseguir un nivel de seguridad altamente satisfactorio, que reduzca al mínimo los riesgos a los que se está expuesto y el impacto que ocasionarían si efectivamente se produjeran.

1.1.1. ¿Por qué se necesita seguridad de la información?

La información y los procesos, sistemas y redes de apoyo son activos comerciales importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, el flujo de caja, rentabilidad, observancia legal e imagen comercial.

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

1.2. Norma ISO/IEC 27001

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo.

Este es un estándar preparado para proveer un modelo de establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un Sistema

de Gestión de Seguridad de la Información documentado; en el contexto de los riesgos específicos de las actividades de la organización.

El Enfoque a Procesos para la gestión de seguridad de información que se presenta en éste Estándar Internacional enfatiza la importancia de:

- **Entender los requerimientos de seguridad de una organización y la necesidad de establecer políticas y objetivos para la seguridad de la información.**
- **Implementar y operar controles para manejar la los riesgos de seguridad de la información.**
- **Monitorear y revisar el rendimiento del Sistema de Gestión de seguridad de la Información**
- **Mejoramiento continúo.**

Éste estándar adopta un modelo "Planear-Hacer-Revisar-Actuar" que se aplica para estructurar todos los procesos del SGSI.

1.2.1. Ciclo de mejora continua

Metodología PDCA / PHVA

Para establecer y gestionar un sistema de gestión de la seguridad de la información se utiliza el ciclo PDCA (conocido también como ciclo Deming), tradicional en los sistemas de gestión de la calidad. El ciclo PDCA es un concepto ideado originalmente por Walter Andrew Shewhart, pero adaptado a lo largo del tiempo por algunos de los más sobresalientes personajes del mundo de la calidad. Esta metodología ha demostrado su aplicabilidad y ha permitido establecer la mejora continua en organizaciones de todas clases.

El modelo PDCA o "Planificar-Hacer-Verificar-Actuar" (*Plan-Do-Check-Act*, de sus siglas en inglés), tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización:

• ***Planificar.*** Esta fase se corresponde con establecer el SGSI. Se planifica y diseña el programa, sistematizando las políticas a aplicar en la organización, cuáles son los fines a alcanzar y en qué ayudarán a lograr los objetivos de negocio, qué medios se utilizarán para ello, los procesos de negocio y los activos que los soportan, cómo se enfocará el análisis de riesgos y los criterios que se seguirán para gestionar las contingencias de modo coherente con las políticas y objetivos de seguridad.

• ***Hacer.*** Es la fase en la que se implementa y pone en funcionamiento el SGSI. Las políticas y los controles escogidos para cumplirlas se implementan mediante recursos

técnicos, procedimientos o ambas cosas a la vez, y se asignan responsables a cada tarea para comenzar a ejecutarlas según las instrucciones.

• ***Verificar.*** Esta fase es la de monitorización y revisión del SGSI. Hay que controlar que los procesos se ejecutan como se ha establecido, de manera eficaz y eficiente, alcanzando los objetivos definidos para ellos. Además, hay que verificar el grado de cumplimiento de las políticas y procedimientos, identificando los fallos que pudieran existir y, hasta donde sea posible, su origen, mediante revisiones y auditorías.

• ***Actuar.*** Es la fase en la que se mantiene y mejora el SGSI, decidiendo y efectuando las acciones preventivas y correctivas necesarias para rectificar los fallos, detectados en las auditorías internas y revisiones del SGSI, o cualquier otra información relevante para permitir la mejora permanente del SGSI.

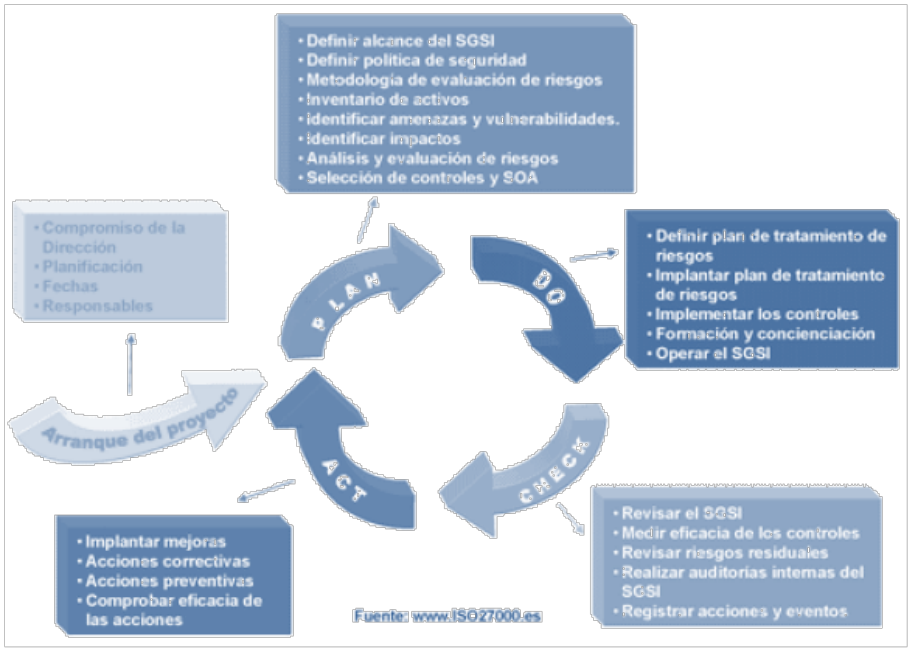


Figura 1-1: Ciclo PDCA

La mejora continua es un proceso en sí mismo. Debe entenderse como la mejora progresiva de los niveles de eficiencia y eficacia de una organización en un proceso continuo de aprendizaje, tanto de sus actividades como de los resultados propios. Dado que la norma se encuentra enfocada hacia la mejora continua, es un esfuerzo innecesario tratar de implementar un SGSI perfecto en un primer proyecto de este tipo. El objetivo debería ser diseñar un SGSI que se ajuste lo más posible a la realidad de la organización, que contemple las medidas de seguridad mínima e imprescindible para proteger la información y cumplir con la norma, pero que consuma pocos recursos e introduzca el menor número de cambios posibles. De esta manera, el SGSI se podrá integrar de una forma no traumática en la operativa habitual de la organización,

dotándola de herramientas con las que hasta entonces no contaba que puedan demostrar su eficacia a corto plazo.

La aceptación de este primer SGSI es un factor de éxito fundamental. Permitirá a la organización ir mejorando su seguridad paulatinamente y con escaso esfuerzo.

1.3. Desarrollo de Software a la Medida

Consiste en que, de manera general, el ciclo de vida de las aplicaciones informáticas (software) va variando, dependiendo de las exigencias, requerimientos y funciones de las empresas clientes. Son, como el término lo indica, a su medida. No sigue un estándar generalizado, sino que se ajusta a un proceso de modelado y desarrollo de acuerdo al cliente.
El proceso implica determinados componentes, descritos en el siguiente diagrama:

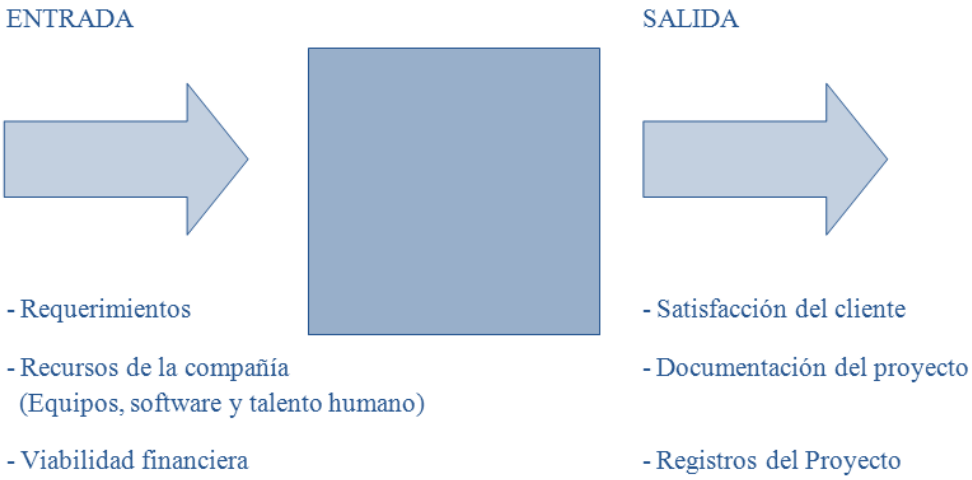
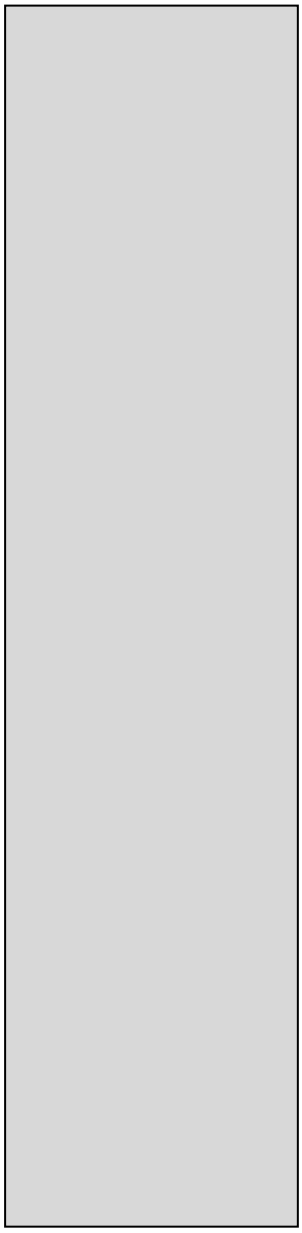


Figura 1-2: Proceso de desarrollo de software a la medida



CAPÍTULO 2
LA EMPRESA

2. LA EMPRESA

2.1. Historia

En 1999 un grupo de Consultores Internacionales de Software decidió crear una empresa con el fin de ofrecer soluciones completas a requerimientos crecientes en los diferentes segmentos del mercado. Su principal característica es la gran experiencia adquirida en instituciones públicas, comerciales, bancarias y educativas, la cual le permite contar con un equipo de trabajo que cubre a cabalidad con todas las expectativas del mercado.

2.2. Misión

Satisfacer a nuestros clientes, a través de la implementación de soluciones tecnológicas, basada en estándares internacionales de gestión de servicio.

2.3. Visión

Ser líder en el sector de Tecnologías de Información ecuatoriano y una de las 30 primeras en el contexto Latinoamericano, impulsando la competitividad y el desarrollo tecnológico a nivel empresarial y humano.

2.4. Valores

Compromiso, Responsabilidad, Proactividad, Trabajo en equipo, Creatividad, Eficiencia, Disciplina, Honestidad, Respeto, Moralidad.

2.5. Productos y Servicios

Oracle
Corlasosa es una empresa *Partner* de Oracle Corporation desde el 2001, por lo cual cuenta con experiencias en asesorías de licenciamientos.

Su personal cuenta con los certificados Oracle Technology Support Specialist, Sales Specialist, OCP Database y OCP Aplication Server los cuales nos otorgan un alto nivel de conocimientos.

Entre los Servicios Oracle se encuentran:

- **Asesoría en Licenciamiento de productos.**

- **Asesoría para definir la Arquitectura de su plataforma Oracle.**
- **Implementación de Opciones de Oracle Enterprise: Particionamiento, Auditoria, OLAP.**
- **Instalación y configuración de productos ORACLE.**
- **Afinamiento de Base de Datos y aplicaciones bajo ORACLE.**
- **Migración de Productos ORACLE.**
- **Implementación de Real Application Cluster.**
- **Instalación y configuración de Sistemas Operativos: UNIX, Solaris, AIX, Linux.**

SEED

La plataforma SEED, se presentó como una necesidad de contar con una plataforma web sobre la cual se puedan incluir nuevos módulos con esto se evita tener un folio en blanco para proyectos futuros.

En su primera versión existió un esqueleto web hecho con tecnologías no estándares (Struts, Hibernate), en la actualidad se realizará un desarrollo con tecnologías incluidas en el estándar JEE con los cual nos beneficiaremos de las bondades de dicha plataforma.

El proyecto SEED es una plataforma web que está implementada con tecnología java especificación JEE 5

Desarrollo a la medida

Con su equipo de consultores cuentan con una amplia gama de conocimientos de productos y tecnologías. A continuación se detallan los productos en que su personal tiene experiencia:

Análisis y Diseño:	UML, Casos de Uso y Modelo Entidad/Relación
Base de Datos:	Oracle MySQL Sybase SQL Server
Lenguajes de Programación:	J2EE.- Java, Servlets, JavaScripts, JSP, JSF, ADF, JDBC, Javanet, Struts, Hibernate y Administración de Persistencia(Toplinks). Shell, AWK, XML, Ajax, PHP, SQL y Oracle PLSQL. Lenguaje C, C++, , Perl
Herramientas de Desarrollo:	Visual Basic, Cristal Reports Oracle Developer, JDeveloper, Eclipse, Netbeans,

PowerBuilder, PeopleSoft
.NET, VB.Net, ASP.Net, C#

Se han implementado importantes proyectos para varios tipos de Industrias, destacando: Automotriz, Telecomunicaciones, Alimentación, Servicio, Química, Manufacturera y Financiera.

2.6. Situación Inicial

Actualmente la empresa objeto del presente proyecto se encuentra en proceso de obtener la certificación ISO 9001:2008. Los directivos están de acuerdo en que, aprovechando la actual situación, implementar las respectivas seguridades sobre la información de desarrollo, con el objetivo de alcanzar ambas certificaciones en mediano plazo, lo que les permitirá obtener un mejor nivel de competencia en el mercado. Los que conforman la empresa están conscientes en que ellos tienen su propia gestión de seguridad de información, pero que el riesgo de fuga de información está latente, ya que el ambiente de disposición a nivel de hardware puede permitir tales riesgos.

2.7. Organigrama

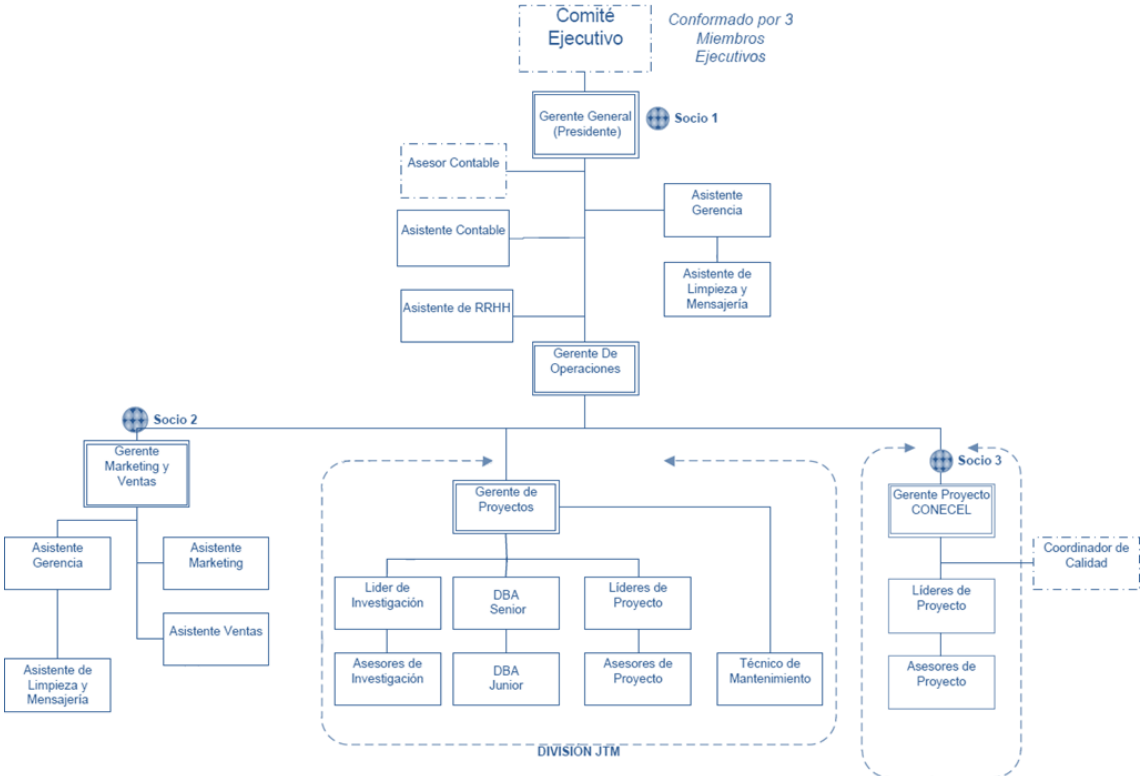
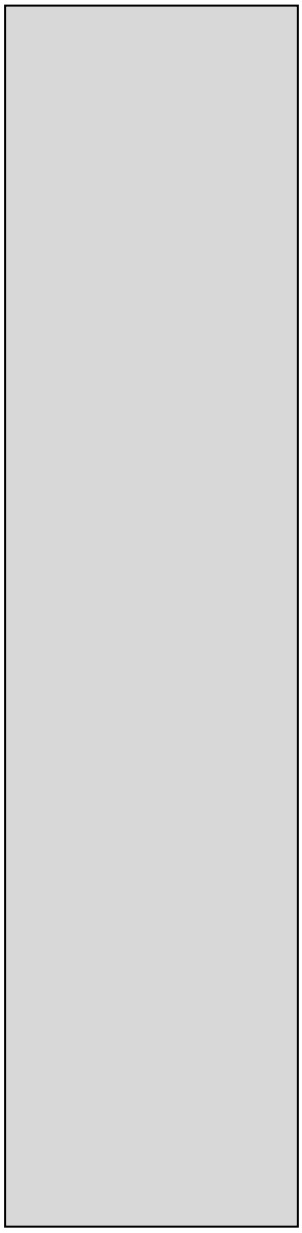


Figura 2-1: Organigrama CORLASOSA



CAPÍTULO 3
ETAPA DE PLANIFICACIÓN

3. ETAPA DE PLANIFICACIÓN

3.1. Alcance del SGSI dentro de la Empresa

En la empresa se considera prioritario a nivel interno:

- **La mejora de su competitividad, dentro del mercado en donde desarrolla su actividad.**
- **El aumento de la rentabilidad, mejorando los procesos. Para alcanzar estos objetivos ha establecido como primer paso la implementación de un sistema de Calidad según la Norma ISO 9001:2008 (en proceso de obtención de la certificación). Este sistema ha sido limitado al proceso de Desarrollo a la Medida, siendo éste el proceso clave de la empresa.**
- **El cumplimiento de estándares internacionales de servicio, para lo cual se propone la implementación del Sistema de Gestión de Seguridad de la Información, según la Norma ISO/IEC 27001. Este sistema comprende diversos dominios de cobertura, que se detallan en la siguiente figura.**

Figura 3-1: Esquema de Dominios del SGSI

El alcance del SGSI dentro de la empresa está enfocado hacia el proceso de **Desarrollo de Software a la Medida**. Este proceso consiste en el diseño e implementación de soluciones de acuerdo a los requerimientos de los clientes. Está implementado dentro del departamento de Proyectos de la empresa y se lleva a cabo en ambos locales.

Mediante la guía de la ISO / IEC 27002 (Mejores prácticas. Figura Nª2: Dominios) determinamos que el dominio a trabajar es: ***12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información*** que se implementará para el proceso de

Desarrollo de Software a la Medida. Los objetivos de control a contemplar son los siguientes:

a. **Requerimientos de seguridad de los sistemas de información**
    - **Análisis y especificación de los requerimientos de seguridad**
b. **Procesamiento correcto en las aplicaciones**
    - **Validación de la input data**
    - **Control del procesamiento interno**
    - **Integridad del mensaje**
    - **Validación de la output data**
c. **Controles criptográficos**
    - **Política sobre el uso de controles criptográficos**
    - **Gestión de claves**
d. **Seguridad de los archivos del sistema**
    - **Control del software operacional**
    - **Protección de la data del sistema**
    - **Control de acceso al código fuente del programa**
e. **Seguridad en los procesos de desarrollo y soporte**
    - **Procedimientos del control del cambio**
    - **Revisión técnica de la aplicación después de cambios en el sistema**
    - **Restricciones sobre los cambios en los paquetes de software**
    - **Filtración de información**
    - **Desarrollo de software abastecido externamente**
f. **Gestión de la Vulnerabilidad Técnica**
    - **Control de las vulnerabilidades técnicas**

3.2. Metodología a utilizar

La metodología a utilizar para determinar el enfoque del análisis y los criterios de gestión de riesgos en el SGSI es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas).

3.2.1. MAGERIT

La Metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se

prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo.

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos y por ello han aparecido multitud de guías informales, aproximaciones metódicas y herramientas de soporte todas las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

3.2.2. Objetivos de MAGERIT

Directos

a. **Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo**
b. **Ofrecer un método sistemático para analizar tales riesgos**
c. **Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control**

Indirectos

a. **Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso**

3.2.3. Terminología usada en MAGERIT

Modelo de valor
Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos
Relación de las amenazas a que están expuestos los activos.

Evaluación de salvaguardas
Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo
Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias
Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

Plan de seguridad
Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.

Seguridad (de la Información)
Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

Disponibilidad: o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad: o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

Autenticidad (de quién hace uso de los datos o servicios): o que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores. Contra la autenticidad se dan suplantaciones y engaños que buscan realizar un fraude. La autenticidad es la base para poder luchar contra el repudio y, como tal,

fundamenta el comercio electrónico o la administración electrónica, permitiendo confiar sin papeles ni presencia física.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre un sistema de tecnología de la información sean asociadas de modo inequívoco a un individuo o entidad

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema:

Análisis de riesgos: proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Sabiendo lo que podría pasar, hay que tomar decisiones:

Gestión de riesgos: selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio.

3.3. Estructuración del proyecto MAGERIT

Participantes

Durante el desarrollo del proyecto AGR (Análisis y Gestión de Riesgos), desde su inicio a su terminación, se identifican los siguientes órganos colegiados:

Comité de Dirección

El perfil requerido para este grupo de participantes incluye a personas con un nivel alto en la dirección de la Organización, conocimiento de los objetivos estratégicos y de negocio que se persiguen y autoridad para validar y aprobar cada uno de los procesos realizados durante el desarrollo del proyecto. En el presente proyecto el Comité de Dirección lo conformará el ***Comité Ejecutivo*** de la empresa.

Comité de Seguimiento

Está constituido por los responsables de las unidades afectadas por el proyecto; así como por los responsables de la informática y de la gestión dentro de dichas unidades.

El Comité de Seguimiento está conformado por el ***Gerente de Marketing y Ventas*** y el ***Gerente de Proyectos Conecel*** de la empresa.

Equipo de proyecto

Formado por personal experto en tecnologías y sistemas de información y personal técnico cualificado del dominio afectado, con conocimientos de gestión de seguridad en general y de la aplicación de la metodología de análisis y gestión de riesgos en particular. Si el proyecto se hace con asistencia técnica mediante contratación externa, el subsiguiente personal especialista en seguridad de sistemas de información se integrará en este equipo de proyecto.

El Equipo de proyecto será el mismo ***equipo que sustenta el presente proyecto de tesis***.

Grupos de Interlocutores

Está formado por usuarios representativos dentro de las unidades afectadas por el proyecto. En este caso serán los ***miembros de las áreas involucradas en el proceso de Desarrollo de Software a la Medida (Proyectos)***.

Además de dichos órganos colegiados, hay que identificar algunos roles singulares:

Promotor

Es aquél que propone el proyecto de AGR. Es una figura singular que lidera las primeras tareas del proyecto, perfilando su oportunidad y alcance para lanzar el proyecto AGR propiamente dicho. Esta función corresponderá al ***director del presente proyecto de tesis***.

Director del Proyecto

Debe ser un directivo de alto nivel, con responsabilidades en seguridad dentro de la Organización, de sistemas de información o, en su defecto, de planificación, de coordinación o de materias, servicios o áreas semejantes. Esta función la ejecutará el ***Gerente de Operaciones Conecel***.

Enlace operacional

Será una persona de la Organización con buen conocimiento de las personas y de las unidades implicadas en el proyecto AGR, que tenga capacidad para conectar al equipo de proyecto con el grupo de usuarios. Esta función la ejecutará el ***Gerente de Operaciones Marketing y Ventas***.

3.4. Plan de Trabajo MAGERIT

Proceso/Actividad	Participantes	Recursos	Tiempo estimado
Proceso 1: Planificación			
Actividad 1.1: Estudio de oportunidad	Promotor	Norma ISO 27001, Ficha de la empresa	1 semana
Actividad 1.2: Determinación del alcance del proyecto	Equipo de Proyecto, Director de Proyecto	Norma ISO 27001, Ficha de la empresa	2 días
Actividad 1.3: Planificación del proyecto	Equipo de Proyecto, Comité de Dirección, Enlace Operacional	Relación de participantes	3 días
Actividad 1.4: Lanzamiento del proyecto	Equipo de Proyecto	Catálogo de tipos de activos, Criterios de evaluación	2 días
Proceso 2: Análisis de riesgos			
Actividad 2.1: Caracterización de los activos	Equipo de Proyecto, Interlocutores	Inventario de activos, Modelo de valor	1 semana
Actividad 2.2: Caracterización de las amenazas	Equipo de Proyecto, Interlocutores	Mapa de riesgo	1 semana
Actividad 2.3: Caracterización de las salvaguardas	Equipo de Proyecto, Interlocutores	Procedimientos operativos, contratos y acuerdos	3 días
Actividad 2.4: Estimación del estado de riesgo	Equipo de Proyecto, Interlocutores	Mapa de riesgo e informe de salvaguardas	2 días
Proceso P3: Gestión de riesgos			
Actividad 3.1: Toma de decisiones	Equipo de Proyecto, Comité de Dirección y Comité de Seguimiento	Resultados de proceso anterior, legislación aplicable, contratos y acuerdos	2 días

Actividad 3.2: Plan de seguridad	Equipo de Proyecto	Plan de seguridad	3 días
Actividad A3.3: Ejecución del plan	Departamento de Proyectos de la Empresa	Salvaguardas implantadas, normas de uso y operación	hasta la próxima revisión

Tabla 3-1: Plan de Trabajo MAGERIT

3.5. Catálogo de Tipos de Activos

Se definen los siguientes tipos de activos, de acuerdo al dominio que se ha establecido:

[S] Servicios
- [ext] a usuarios externos (bajo una relación contractual)

[D] Datos/Información
- [com] datos de interés comercial
- [source] código fuente
- [exe] código ejecutable
- [conf] datos de configuración
- [log] registro de actividad (log)
- [test] datos de prueba

[S] Aplicaciones (software)
- [std] estándar (off the shelf)

3.6. Criterios de valoración de Activos

Nivel de valoración	Valor
10	Muy alto
9	Muy alto
8	Alto
7	Alto
6	Medio
5	Medio
4	Bajo
3	Bajo
2	Muy bajo
1	Muy bajo

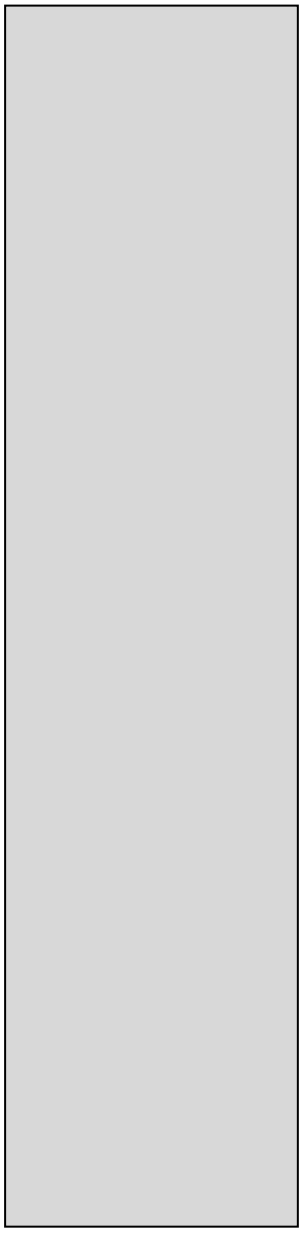
Dimensiones
Integridad
Disponibilidad
Confidencialidad
Autenticación
Datos
Servicios
Trazabilidad
Datos
Servicios

Tabla 3-2: Criterios de valoración de Activos

3.7. Criterios de valoración de Impacto y Riesgo

Nivel de valoración (en porcentaje)	Impacto	Frecuencia	Riesgo (Impacto * Frecuencia)
100	Muy alto	Siempre	Muy alto
90	Muy alto	Muy alto	Muy alto
80	Alto	Muy alto	·
70	Alto	·	grave
60	Medio	·	·
50	Medio	·	·
40	Bajo	·	apreciable
30	Bajo	·	·
20	Muy bajo	·	·
10	Muy bajo	Menor frecuencia	Menor riesgo (asumible)

Tabla 3-3: Criterios de valoración de Impacto y Riesgo



CAPÍTULO 4
ANÁLISIS DE RIESGOS

4. ANÁLISIS DE RIESGOS

4.1. Caracterización de activos

4.1.1. Identificación de activos

A continuación se detalla los activos actuales de la Empresa que están dentro del Dominio 12, "Adquisición, Desarrollo y Mantenimiento de Sistemas de Información"

- **Servicios:**
    - Desarrollo de software a la medida

      Considérese este activo como la principal actividad económica y motivo de existencia de la Empresa, ya que sin este activo, la Empresa no existiría.

- **Datos**
    - Datos de entrada
    - Documento impreso de entrada
    - Procesamiento interno del sistema
    - Mensaje del sistema
    - Claves del sistema
    - Código fuente
    - Programas del sistema
    - Datos de prueba

- **Software**
    - Microsoft Windows XP SP2
    - Adobe Reader v. 9.4.4 Español
    - Apache Tomcat v. 5.0
    - AVG internet Security 2011
    - Beyond Compare v. 3.2.3
    - Edit Plus v. 3
    - Windows Internet Explorer 7
    - FileZilla client v. 3.2.1
    - Microsoft Outlook 2007
    - Microsoft Office Enterprise 2007
    - MyEclipse v. 5.5.1
    - Oracle DB 10g Express Edition
    - Oracle Virtual Box
    - PL/SQL Developer
    - VM Ware Player
    - Spark v. 2.5.8

4.1.2. Inventario de Activos

Activo	Descripción	Versión	Responsable
CLS_S_0001	DESARROLLO DE SOFTWARE A LA MEDIDA	-	Gerente de Operaciones
CLS_DT_0001	DATOS DE ENTRADA	-	Gerente de Proyectos
CLS_DT_0002	DOCUMENTO IMPRESO DE ENTRADA	-	Gerente de Proyectos
CLS_DT_0003	PROCESAMIENTO INTERNO DEL SISTEMA	-	Gerente de Proyectos
CLS_DT_0004	MENSAJE DEL SISTEMA	-	Gerente de Proyectos
CLS_DT_0005	CLAVES DEL SISTEMA	-	Gerente de Proyectos
CLS_DT_0006	CODIGO FUENTE	-	Gerente de Proyectos
CLS_DT_0007	PROGRAMAS DEL SISTEMA	-	Gerente de Proyectos
CLS_DT_0008	DATOS DE PRUEBA	-	Gerente de Proyectos
CLS_SW_0001	MICROSOFT WINDOWS XP SP2	XP SP2	Gerente de Operaciones
CLS_SW_0002	ADOBE READER V. 9.4.4 ESPAÑOL	9.4.4	Gerente de Operaciones
CLS_SW_0003	APACHE TOMCAT V. 5.0	5.0	Gerente de Operaciones
CLS_SW_0004	AVG INTERNET SECURITY 2011	2011	Gerente de Operaciones
CLS_SW_0005	BEYOND COMPARE V. 3.2.3	3.2.3	Gerente de Operaciones
CLS_SW_0006	EDIT PLUS V. 3	3	Gerente de Operaciones
CLS_SW_0007	WINDOWS INTERNET EXPLORER 7	7	Gerente de Operaciones
CLS_SW_0008	FILEZILLA CLIENT V. 3.2.1	3.2.1	Gerente de Operaciones
CLS_SW_0009	MICROSOFT OUTLOOK 2007	2007	Gerente de Operaciones
CLS_SW_0010	MICROSOFT OFFICE ENTERPRISE 2007	2007	Gerente de Operaciones
CLS_SW_0011	MYECLIPSE V. 5.5.1	5.5.1	Gerente de Operaciones
CLS_SW_0012	ORACLE DB 10G EXPRESS EDITION	10G	Gerente de Operaciones
CLS_SW_0013	ORACLE VIRTUAL BOX	-	Gerente de Operaciones
CLS_SW_0014	PL/SQL DEVELOPER	-	Gerente de Operaciones
CLS_SW_0015	VMWARE PLAYER	-	Gerente de Operaciones
CLS_SW_0016	SPARK V. 2.5.8	2.5.8	Gerente de Operaciones

Tabla 4-1: Inventario de Activos

4.1.3. Valoración de Activos (Modelo de valor)

LEYENDA: I (Integridad), D (Disponibilidad), C (Confidencialidad), AS (Autenticidad del Servicio), TS (Trazabilidad del Servicio), AD (Autenticidad de los Datos), TD (Trazabilidad de los datos), T (Total)

Activo	Descripción	I	D	C	AS	TS	AD	TD	T
CLS_S_0001	DESARROLLO DE SOFTWARE A LA MEDIDA	9	9	9	9	9	-	-	45
CLS_DT_0001	DATOS DE ENTRADA	8	9	9	-	-	8	8	42
CLS_DT_0002	DOCUMENTO IMPRESO DE ENTRADA	8	9	9	-	-	8	8	42
CLS_DT_0003	PROCESAMIENTO INTERNO DEL SISTEMA	8	9	9	-	-	8	8	42
CLS_DT_0004	MENSAJE DEL SISTEMA	8	9	9	-	-	8	8	42
CLS_DT_0005	CLAVES DEL SISTEMA	8	9	9	-	-	8	8	42
CLS_DT_0006	CODIGO FUENTE	8	9	9	-	-	8	8	42
CLS_DT_0007	PROGRAMAS DEL SISTEMA	8	9	9	-	-	8	8	42
CLS_DT_0008	DATOS DE PRUEBA	8	9	9	-	-	8	8	42
CLS_SW_0001	MICROSOFT WINDOWS XP SP2	7	7	6	-	-	7	5	32
CLS_SW_0002	ADOBE READER V. 9.4.4 ESPAÑOL	5	5	4	-	-	5	3	22
CLS_SW_0003	APACHE TOMCAT V. 5.0	5	5	4	-	-	5	3	22
CLS_SW_0004	AVG INTERNET SECURITY 2011	5	5	4	-	-	5	3	22
CLS_SW_0005	BEYOND COMPARE V. 3.2.3	5	5	4	-	-	5	3	22
CLS_SW_0006	EDIT PLUS V. 3	5	5	4	-	-	5	3	22
CLS_SW_0007	INTERNET EXPLORER 7	5	5	4	-	-	5	3	22

CLS_SW_0008	FILEZILLA CLIENT V. 3.2.1	5	5	4	-	-	5	3	22
CLS_SW_0009	MICROSOFT OUTLOOK 2007	5	5	4	-	-	5	3	22
CLS_SW_0010	MICROSOFT OFFICE ENTERPRISE 2007	5	5	4	-	-	5	3	22
CLS_SW_0011	MYECLIPSE V. 5.5.1	5	5	4	-	-	5	3	22
CLS_SW_0012	ORACLE DB 10G EXPRESS EDITION	5	5	4	-	-	5	3	22
CLS_SW_0013	VIRTUAL BOX	5	5	4	-	-	5	3	22
CLS_SW_0014	PL/SQL DEVELOPER	5	5	4	-	-	5	3	22
CLS_SW_0015	VMWARE PLAYER	5	5	4	-	-	5	3	22
CLS_SW_0016	SPARK V. 2.5.8	5	5	4	-	-	5	3	22

Tabla 4-2: Tabla de activos valorada

4.2. Caracterización de amenazas

4.2.1. Identificación de amenazas

[I] De origen industrial
[I.5] Avería de origen físico o lógico
Aplica a:
[SW] aplicaciones (software)
Dimensiones:
[D] disponibilidad
[T_S] trazabilidad de los servicios
[T_D] trazabilidad de los datos
Descripción:
Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

4.2.2. Identificación de errores

[E.1] Errores de los usuarios
Aplica a:
[S] servicios
[D] datos / información
[SW] aplicaciones (software)
Dimensiones:
[I] integridad
[D] disponibilidad
Descripción:
Equivocaciones de las personas cuando usan los servicios, datos, etc.

[E.2] Errores del administrador
Aplica a:
[S] servicios
[D] datos / información
[SW] aplicaciones (software)
[HW] equipos informáticos (hardware)
[COM] redes de comunicaciones

Dimensiones:
[D] disponibilidad
[I] integridad
[C] confidencialidad
[A_S] autenticidad del servicio
[A_D] autenticidad de los datos
[T_S] trazabilidad del servicio
[T_D] trazabilidad de los datos

Descripción:
Equivocaciones de personas con responsabilidades de instalación y operación

[E.3] Errores de monitorización *(log)*
Aplica a:
[S] servicios
[D] datos / información
[SW] aplicaciones (software)
Dimensiones:
[T_S] trazabilidad del servicio
[T_D] trazabilidad de los datos

Descripción:
Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.

[E.4] Errores de configuración
Aplica a:
[S] servicios
[D] datos / información
[SW] aplicaciones (software)
Dimensiones:
[D] disponibilidad
[I] integridad
[C] confidencialidad
[A_S] autenticidad del servicio
[A_D] autenticidad de los datos
[T_S] trazabilidad del servicio
[T_D] trazabilidad de los datos
Descripción:
Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

[E.8] Difusión de software dañino
Aplica a:
[SW] aplicaciones (software)
Dimensiones:
[D] disponibilidad
[I] integridad
[C] confidencialidad
[A_S] autenticidad del servicio
[A_D] autenticidad de los datos
[T_S] trazabilidad del servicio
[T_D] trazabilidad de los datos
Descripción:
Propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.

[E.9] Errores de [re-]encaminamiento
Aplica a:
[S] servicios
[SW] aplicaciones (software)

Dimensiones:

[C] confidencialidad
[I] integridad
[A_S] autenticidad del servicio
[T_S] trazabilidad del servicio

Descripción:

Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información por la vía equivocada a un destino equivocado; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.

[E.10] Errores de secuencia

Aplica a:

[S] servicios
[SW] aplicaciones (software)

Dimensiones:

[I] integridad

Descripción:

Alteración accidental del orden de los mensajes transmitidos.

[E.14] Escapes de información

Aplica a:

[D] datos / información
[SW] aplicaciones (software)

Dimensiones:

[C] confidencialidad

Descripción:

La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.

[E.15] Alteración de la información

Aplica a:

[D] datos / información

Dimensiones:

[I] integridad

Descripción:

Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.16] Introducción de información incorrecta

Aplica a:

[D] datos / información

Dimensiones:

[I] integridad

Descripción:

Inserción accidental de información incorrecta. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.17] Degradación de la información

Aplica a:

[D] datos / información

Dimensiones:

[I] integridad

Descripción:

Degradación accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.18] Destrucción de información

Aplica a:

[D] datos / información

Dimensiones:

[D] disponibilidad

Descripción:

Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.19] Divulgación de información

Aplica a:

[D] datos / información

Dimensiones:

[C] confidencialidad

Descripción:

Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.

[E.20] Vulnerabilidades de los programas (software)

Aplica a:

[SW] aplicaciones (software)

Dimensiones:

[I] integridad

[D] disponibilidad

[C] confidencialidad

Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.

[E.21] Errores de mantenimiento / actualización de programas (software)

Aplica a:

[SW] aplicaciones (software)

Dimensiones:

[I] integridad

[D] disponibilidad

Descripción:

Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[E.24] Caída del sistema por agotamiento de recursos

Aplica a:

[S] servicios

Dimensiones:

[D] disponibilidad

Descripción:

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

4.2.3. Porcentajes generales de impacto y riesgo sobre los activos (Mapa de riesgo)

Activo	Porcentaje General de Impacto	Porcentaje General de Frecuencia	Porcentaje General de Riesgo
CLS_S_0001: DESARROLLO DE SOFTWARE A LA MEDIDA	71,05	71,58	71,32
CLS_DT_0001: DATOS DE ENTRADA	47,21	17,11	32,16
CLS_DT_0002: DOCUMENTO IMPRESO DE ENTRADA	47,21	17,11	32,16
CLS_DT_0003: PROCESAMIENTO INTERNO DEL SISTEMA	47,21	17,11	32,16
CLS_DT_0004: MENSAJE DEL SISTEMA	47,21	17,11	32,16
CLS_DT_0005: CLAVES DEL SISTEMA	47,21	17,11	32,16
CLS_DT_0006: CODIGO FUENTE	47,21	17,11	32,16
CLS_DT_0007: PROGRAMAS DEL SISTEMA	47,21	17,11	32,16
CLS_DT_0008: DATOS DE PRUEBA	47,21	17,11	32,16
CLS_SW_0001: MICROSOFT WINDOWS XP SP2	42,19	15,00	28,59
CLS_SW_0002: ADOBE READER V. 9.4.4 ESPAÑOL	28,30	15,00	21,65
CLS_SW_0003: APACHE TOMCAT V. 5.0	28,30	15,00	21,65
CLS_SW_0004: AVG INTERNET SECURITY 2011	28,30	15,00	21,65
CLS_SW_0005: BEYOND COMPARE V. 3.2.3	28,30	15,00	21,65
CLS_SW_0006: EDIT PLUS V. 3	28,30	15,00	21,65
CLS_SW_0007: WINDOWS INTERNET EXPLORER 7	28,30	15,00	21,65
CLS_SW_0008: FILEZILLA CLIENT V. 3.2.1	28,30	15,00	21,65
CLS_SW_0009: MICROSOFT OUTLOOK 2007	28,30	15,00	21,65
CLS_SW_0010: MICROSOFT OFFICE ENTERPRISE 2007	28,30	15,00	21,65
CLS_SW_0011: MYECLIPSE V. 5.5.1	28,30	15,00	21,65
CLS_SW_0012: ORACLE DB 10G EXPRESS EDITION	28,30	15,00	21,65

CLS_SW_0013: ORACLE VIRTUAL BOX	28,30	15,00	21,65
CLS_SW_0014: PL/SQL DEVELOPER	28,30	15,00	21,65
CLS_SW_0015: VMWARE PLAYER	28,30	15,00	21,65
CLS_SW_0016: SPARK V. 2.5.8	28,30	15,00	21,65

Tabla 4-3: Porcentaje general de las amenazas sobre los activos

4.2.4. Relación entre Impacto, Frecuencia y Riesgo sobe los Activos

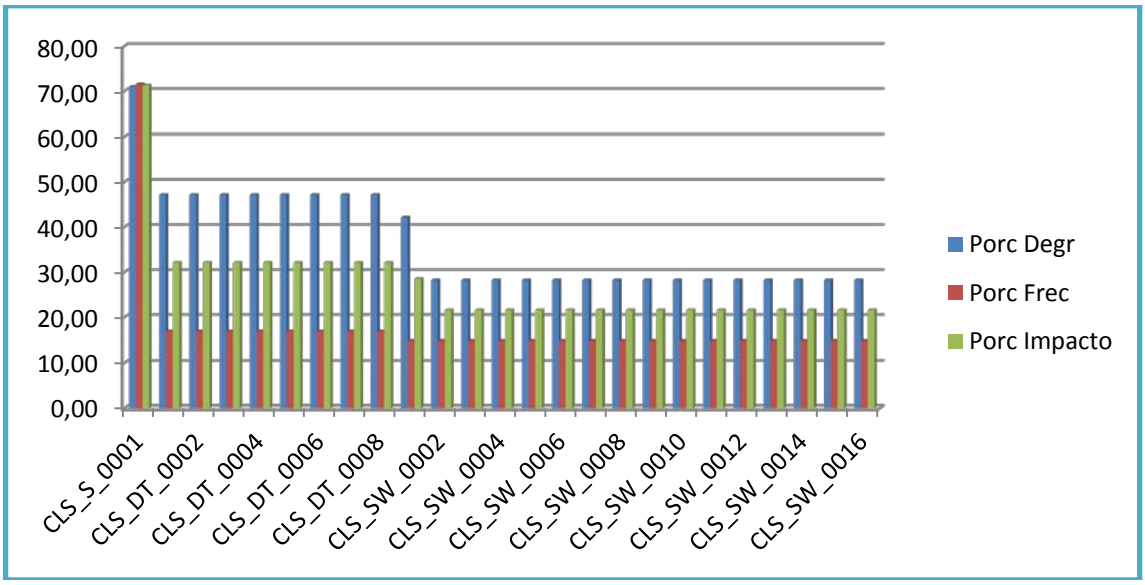


Figura 4-1: Relación entre Degradación, Frecuencia e Impacto sobre Activos

4.3. Caracterización de salvaguardas

Las salvaguardas que se aplican actualmente en la empresa son a nivel reglamentario y contractual, principalmente.

4.3.1. Reglamento Interno de la Compañía

Obliga a los trabajadores a cuidar y usar adecuadamente los elementos de trabajo que le asignen para el desempeño de funciones, entre estos se encuentran los activos informáticos de la empresa. Asimismo el trabajador debe dar las facilidades para aplicar los procedimientos de control y revisión personal destinados a evitar la sustracción indebida de materiales, objetos o información de la Compañía.

4.3.2. Manuales de Funciones

Estipula entre las funciones y responsabilidades el controlar y verificar las modificaciones o mejoras a programas, con la finalidad un mínimo de impacto en la implementación de la solución de software; y monitorear la implementación del proyecto en producción, para verificar que se cumpla con sus objetivos.

4.3.3. Acuerdos de Confidencialidad

Los acuerdos de confidencialidad aseguran que tanto trabajadores como clientes no divulguen a terceros información concerniente a los servicios que presta la empresa.

4.3.4. Procedimientos no documentados

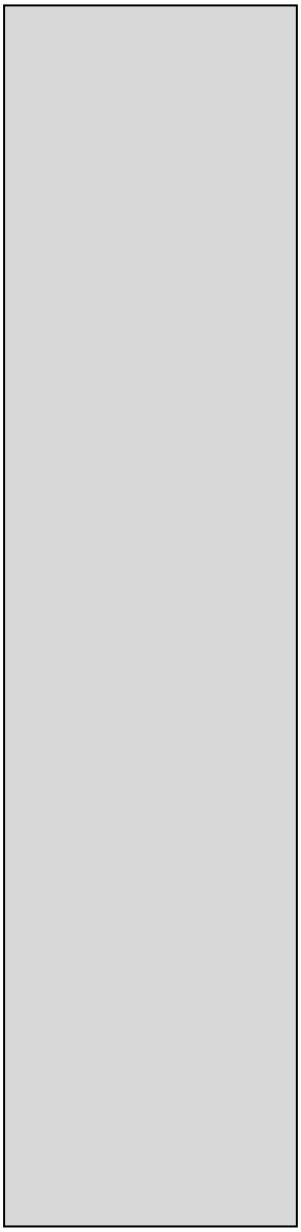
Existen procedimientos no documentados para el control de cambios en los equipos y software usados en el área de proyectos de la empresa. Para esto se deben llenar sendos registros correspondientes para cada cambio.

4.4. Evaluación de Salvaguardas (Cuadro SOA Resumido)

ISO 27001:2005 Controles			Controles Actuales	Comentarios (descripción general de la aplicación)
Dominio	**Sección**	**Control / Objetivos de Control**		
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	12.1	Requerimientos de Seguridad de Sistemas de Información		
	12.1.1	Análisis y Especificaciones de Requerimientos de Seguridad	SI	Centro de datos no hace ningún mantenimiento o apoyo de desarrollo de software de aplicación del sistema. No obstante las mejoras en el hardware (es decir, discos adicionales, etc.) requieren una solicitud de cambio
	12.4	Seguridad de Sistemas de Archivos		
	12.4.1	Control de Software Operacional	SI	Para evitar el control de cambios no autorizados
	12.4.3	Control de acceso a librerías del programa fuente	SI	El código fuente se aloja como una copia de seguridad solamente

	12.5	Seguridad en Procesos de Desarrollo y Soporte		
	12.5.1	Procedimientos de Control de Cambios	SI	Cualquier cambio de centro de datos de activos requiere una solicitud de cambio
	12.5.2	Revisión Técnica de aplicaciones después de cambios en el Sistema Operativo	SI	No es competencia de los centros de datos, pero se debe informar a los dueños de las aplicaciones de los sistemas operativos, cuando se ha producido cambios
	12.5.4	Fuga de Información	SI	Oportunidades para la fuga de información deben evitarse
	12.6	Técnicas en gestión de vulnerabilidades		
	12.6.1	Control de vulnerabilidades técnicas	SI	Vulnerabilidades técnicas deben ser gestionadas

Tabla 4-4: SOA Resumido



CAPÍTULO 5
GESTION DE RIESGOS

5. GESTION DE RIESGOS

5.1. Toma de Decisiones

5.1.1. Calificación de riesgos

Activo	Porcentaje General de Riesgo	Calificación
CLS_S_0001: DESARROLLO DE SOFTWARE A LA MEDIDA	71,32	**grave**
CLS_DT_0001: DATOS DE ENTRADA	32,16	**apreciable**
CLS_DT_0002: DOCUMENTO IMPRESO DE ENTRADA	32,16	**apreciable**
CLS_DT_0003: PROCESAMIENTO INTERNO DEL SISTEMA	32,16	**apreciable**
CLS_DT_0004: MENSAJE DEL SISTEMA	32,16	**apreciable**
CLS_DT_0005: CLAVES DEL SISTEMA	32,16	**apreciable**
CLS_DT_0006: CODIGO FUENTE	32,16	**apreciable**
CLS_DT_0007: PROGRAMAS DEL SISTEMA	32,16	**apreciable**
CLS_DT_0008: DATOS DE PRUEBA	32,16	**apreciable**
CLS_SW_0001: MICROSOFT WINDOWS XP SP2	28,59	**apreciable**
CLS_SW_0002: ADOBE READER V. 9.4.4 ESPAÑOL	21,65	**apreciable**
CLS_SW_0003: APACHE TOMCAT V. 5.0	21,65	**apreciable**
CLS_SW_0004: AVG INTERNET SECURITY 2011	21,65	**apreciable**
CLS_SW_0005: BEYOND COMPARE V. 3.2.3	21,65	**apreciable**
CLS_SW_0006: EDIT PLUS V. 3	21,65	**apreciable**
CLS_SW_0007: WINDOWS INTERNET EXPLORER 7	21,65	**apreciable**

CLS_SW_0008: FILEZILLA CLIENT V. 3.2.1	21,65	**apreciable**
CLS_SW_0009: MICROSOFT OUTLOOK 2007	21,65	**apreciable**
CLS_SW_0010: MICROSOFT OFFICE ENTERPRISE 2007	21,65	**apreciable**
CLS_SW_0011: MYECLIPSE V. 5.5.1	21,65	**apreciable**
CLS_SW_0012: ORACLE DB 10G EXPRESS EDITION	21,65	**apreciable**
CLS_SW_0013: ORACLE VIRTUAL BOX	21,65	**apreciable**
CLS_SW_0014: PL/SQL DEVELOPER	21,65	**apreciable**
CLS_SW_0015: VMWARE PLAYER	21,65	**apreciable**
CLS_SW_0016: SPARK V. 2.5.8	21,65	**apreciable**

Tabla 5-1: Inventario de Activos calificado

5.2. Plan de Seguridad

5.2.1. Política de Seguridad

En CORLASOSA la seguridad de la información es una prioridad, por lo que se busca el adecuado control y mitigación de los riesgos que involucra la prestación de servicios de desarrollo a la medida, principal actividad de la empresa; bajo el estándar internacional del Sistema de Gestión de Seguridad de la Información ISO 27001, y el cumplimiento de objetivos de control mediante la mejora continua de la seguridad organizacional.

5.2.2. Procedimientos y Controles

Requerimientos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información. Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones comerciales, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso comercial puede ser crucial para la seguridad. Se debieran identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información. Se debieran identificar todos los requerimientos de seguridad en la fase de requerimientos de un proyecto; y debieran ser justificados, acordados y documentados como parte del caso comercial general para un sistema de información.

Análisis y especificación de los requerimientos de seguridad
Control
Los enunciados de los requerimientos comerciales para los sistemas de información nuevos, o las mejoras a los sistemas de información existentes, debieran especificar los requerimientos de los controles de seguridad. Los requerimientos y los controles de seguridad debieran reflejar el valor comercial de los activos de información involucrados, y el daño comercial potencia que podría resultar de una falla o ausencia de seguridad.

Los requerimientos de seguridad para la seguridad de la información y los procesos para implementar la seguridad debieran ser integrados en las primeras etapas de los proyectos de sistemas de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si los productos son comprados, se debiera realizar un proceso de prueba y adquisición formal. Los contratos con el proveedor debieran tratar los requerimientos de seguridad identificados. Cuando la funcionalidad de seguridad de un producto propuesto no satisface el requerimiento especificado entonces se debieran reconsiderar el riesgo introducido y los controles asociados antes de comprar el producto. Donde se suministra funcionalidad adicional y causa un riesgo de seguridad, este debiera ser desactivado o se debiera revisar la estructura de control propuesta para determinar si se puede obtener alguna ventaja de la funcionalidad mejorada disponible.

Información adicional
Si se considera apropiado, por ejemplo por razones de costo, la gerencia puede hacer uso de productos evaluados y certificados independientemente.

Procesamiento correcto en las aplicaciones
Objetivo: Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones. Se debieran diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para asegurar un procesamiento correcto. Estos controles debieran incluir la validación de la input data, procesamiento interno y output data.
Se pueden requerir controles adicionales para los sistemas que procesan, o tienen impacto sobre, la información confidencial, valiosa o crítica. Estos controles se debieran determinar sobre la base de los requerimientos de seguridad y la evaluación del riesgo.

Validación de la input data
Control
Se debiera validar la input data para las aplicaciones para asegurar que esta data sea correcta y apropiada.

Implementación

Se debieran realizar chequeos del input de las transacciones comerciales, la data fija (por ejemplo nombres y direcciones, límites de crédito, números de referencia de los clientes), y tablas de parámetros (por ejemplo; precios de venta, moneda, tasas de cambio, tasa tributaria). Se debieran considerar los siguientes lineamientos:

a. input dual u otros chequeos de data; tales como chequeo de límites o limitar los campos a los rangos específicos de la input data; para detectar los siguientes errores:
    - valores fuera de rango;
    - caracteres inválidos en los campos de data;
    - data incompleta o faltante;
    - exceder los límites superiores e inferiores del volumen de data;
    - data de control no autorizado o inconsistente;
b. revisión periódica del contenido de los campos claves o archivos de data para confirmar su validez e integridad;
c. inspeccionar los documentos de input de la copia impresa en caso de cambios no autorizados (todos los cambios a los documentos de input debieran ser autorizados);
d. procedimientos para responder a los errores de validación;
e. procedimientos para probar la plausibilidad de la input data;
f. definir las responsabilidades de todo el personal involucrado en el proceso de input de data;
g. crear un registro de las actividades involucradas en el proceso de input de data.

Información adicional

Cuando sea aplicable, se debiera considerar el examen y validación automática de la input data para reducir el riesgo de errores y evitar los ataques estándar incluyendo el desbordamiento de la memoria intermedia y la inyección de un código.

Control del procesamiento interno

Control

Los chequeos de validación se debieran incorporar en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.

Implementación

El diseño e implementación de las aplicaciones debiera asegurar que se minimicen los riesgos de fallas en el procesamiento que lleven a la pérdida de la integridad. Las áreas específicas a considerarse incluyen:

a. el uso de funciones agregadas, modificadas y eliminadas para implementar cambios en la data;

b. los procedimientos para evitar que los programas corran en el orden equivocado o corran después de una falla en el procesamiento previo;
c. el uso de programas apropiados para recuperarse de fallas para asegurar el correcto procesamiento de la data;
d. protección contra ataques utilizando excesos/desbordamientos de la memora intermedia.

Se debiera preparar una lista de chequeo apropiada, se debieran documentar las actividades y los resultados se debieran mantener seguros. Los ejemplos de los chequeos que se pueden incorporar incluyen lo siguiente:

a. controles de sesión o lote, para conciliar los saldos del archivo de data después de las actualizaciones de la transacción;
b. controles de saldos, para chequear los saldos de apertura comparándolos con los saldos de cierre anteriores; específicamente:
    - controles corrida-a-corrida;
    - totales de actualización del archivo;
    - controles programa-a-programa;
c. validación de la input data generada por el sistema
d. chequeos de la integridad, autenticidad y cualquier otro dispositivo de seguridad de la data o software cargado o descargado, entre la computadora central y las remotas;
e. totales hash de registros y archivos;
f. chequeos para asegurar que los programas se corran en el momento adecuado;
g. chequeos para asegurar que los programas sean corridos en el orden correcto y terminados en caso de una falla, y que se detenga el procesamiento hasta que se resuelva el problema;
h. crear un registro de las actividades involucradas en el procesamiento.

Información adicional

La data que ha sido correctamente ingresada puede verse corrompida por errores en el hardware, errores en el procesamiento o a través de actos deliberados. Los chequeos de validación requeridos dependerán de la naturaleza de la aplicación y el impacto comercial de cualquier corrupción de la data.

Integridad del mensaje

Control

Se debiera identificar los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, y se debieran identificar e implementar los controles apropiados.

Implementación

Se debiera realizar una evaluación de los riesgos de seguridad para determinar si se requiera la integridad del mensaje y para identificar el método de implementación más apropiado.

Información adicional
Se pueden utilizar técnicas criptográficas como un medio apropiado para implementar la autenticación del mensaje.

Validación de la output data
Control
Se debiera validar la output data de una aplicación para asegurar que el procesamiento de la información almacenada sea el correcto y el apropiado para las circunstancias.

Implementación
La validación del output puede incluir:

a. chequeos de plausibilidad para comprobar si el output data es razonable;
b. conteo de control de conciliación para asegurar el procesamiento de toda la data;
c. proporcionar la información suficiente para un lector o el sistema de procesamiento subsiguiente para determinar la exactitud, integridad, precisión y clasificación de la información;
d. procedimientos para responder a las pruebas de validación de output;
e. definir las responsabilidades de todo el personal involucrado en el proceso de output de data;
f. crear un registro de las actividades en el proceso de validación del output de data.

Información adicional
Típicamente, los sistemas y aplicaciones son elaborados sobre la premisa que si han pasado por la apropiada validación, verificación y prueba; el output siempre será el correcto. Sin embargo, esta premisa no es siempre válida; es decir, aún los sistemas que han sido probados pueden producir output incorrecto en algunas circunstancias.

Controles criptográficos
Objetivo: Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos. Se debiera desarrollar una política sobre el uso de controles criptográficos. Se debiera establecer una gestión clave para sostener el uso de técnicas criptográficas.

Política sobre el uso de controles criptográficos
Control
Se debiera desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.

Implementación

Cuando se desarrolla una política criptográfica se debiera considerar lo siguiente:

a. el enfoque gerencial sobre el uso de los controles criptográficos a través de la organización, incluyendo los principios generales bajo los cuales se debiera proteger la información comercial;
b. en base a la evaluación del riesgo, se debiera identificar el nivel de protección requerido tomando en cuenta el tipo, fuerza y calidad del algoritmo criptográfico requerido;
c. el uso de codificación para la protección de la información confidencial transportada por los medios y dispositivos móviles o removibles o a través de las líneas de comunicación;
d. el enfoque de la gestión de claves, incluyendo los métodos para lidiar con la protección de las claves criptográficas y la recuperación de la información codificada en el caso de claves pérdidas, comprometidas o dañadas;

e. roles y responsabilidades; por ejemplo, quién es responsable de:
    - la implementación de la política;
    - la gestión de claves, incluyendo la generación de claves;
f. los estándares a adoptarse para la implementación efectiva en toda la organización (cuál solución se utiliza para cuáles procesos comerciales);
g. el impacto de utilizar información codificada sobre los controles que se basan en la inspección del contenido (por ejemplo, detección de virus);

Cuando se implementa la política criptográfica de la organización, se debiera considerar las regulaciones y las restricciones nacionales que se podrían aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los problemas del flujo inter-fronteras de la información codificada.

Se pueden utilizar controles criptográficos para lograr diferentes objetivos de seguridad:

a. confidencialidad: utilizando la codificación de la información para proteger la información confidencial o crítica, ya sea almacenada o transmitida;
b. integridad/autenticidad: utilizando firmas digitales o códigos de autenticación del mensaje para proteger la autenticidad e integridad de la información confidencial o crítica almacenada o transmitida;
c. no-repudiación: utilizando técnicas criptográficas para obtener prueba de la ocurrencia o no-ocurrencia de un evento o acción.

Información adicional

La decisión de si es apropiada una solución criptográfica debiera ser vista como parte de un proceso más amplio de evaluación del riesgo y selección de controles. Luego esta evaluación se puede utilizar para determinar si es apropiado un control criptográfico, qué tipo de control se debiera aplicar, y para cuáles propósitos y procesos comerciales.

Es necesaria una política sobre el uso de controles criptográficos para maximizar los beneficios y minimizar los riesgos de utilizar técnicas criptográficas, y evitar el uso inapropiado o incorrecto. Cuando se utilizan firmas digitales, se debiera considerar cualquier legislación relevante, en particular la legislación que describe las condiciones bajo las cuales una firma digital es aceptada legalmente. Se debiera buscar asesoría especialista para identificar el nivel de protección apropiado y definir las especificaciones adecuadas que proporcionarán la protección y el soporte requeridos para la implementación de un sistema de gestión de claves a seguir.

Gestión de claves
Control
Se debiera establecer la gestión de claves para dar soporte al uso de técnicas criptográficas en la organización.

Implementación
Todas las claves criptográficas debieran estar protegidas contra una modificación, pérdida y destrucción. Además, las claves secretas y privadas necesitan protección contra la divulgación no-autorizada. Se debiera proteger físicamente el equipo utilizado para generar, almacenar y archivar las claves.
El sistema de gestión de claves se debiera basar en un conjunto de estándares, procedimientos y métodos seguros acordados para:

a. generar claves para los diferentes sistemas criptográficos y las diversas aplicaciones;
b. generar y obtener certificados de claves públicas;
c. distribuir claves a los usuarios planeados, incluyendo cómo se debieran activar las claves una vez recibidas;
d. almacenar claves, incluyendo cómo los usuarios autorizados obtienen acceso a las claves;
e. cambiar o actualizar las claves incluyendo las reglas sobre cuándo se debieran cambiar las claves y cómo se realiza esto;
f. lidiar con las claves comprometidas;
g. revocar las claves incluyendo cómo se debieran retirar o desactivar las claves; por ejemplo, cuando las claves se han visto comprometidas o cuando el usuario deja la organización (en cuyos casos las claves también debieran ser archivadas);
h. recuperar las claves cuando han sido perdidas o corrompidas como parte de la continuidad y gestión del negocio; por ejemplo, para recuperar la información codificada;
i. archivar las claves; por ejemplo, para la información archivada o respaldada;
j. destruir las claves;
k. registrar y auditar las actividades relacionadas con la gestión de claves.

Para poder reducir la posibilidad de comprometer las claves, se debieran definir las fechas de activación y desactivación para que las claves sólo se puedan utilizar durante

un período de tiempo limitado. El período de tiempo dependerá de las circunstancias bajo las cuales se está utilizando el control criptográfico, y el riesgo percibido. Además del manejo seguro de las claves secretas y privadas, también se debiera considerar la autenticidad de las claves públicas. Este proceso de autenticación se puede realizar utilizando certificados de claves públicas, los cuales normalmente son emitidos por una autoridad de certificación, la cual debiera ser una organización reconocida con controles y procedimientos adecuados para proporcionar el grado de confianza requerido.
Los contenidos de los acuerdos o contratos de nivel de servicio con los proveedores externos de servicios de criptografía; por ejemplo, una autoridad de certificación; debieran abarcar los temas de responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la provisión de los servicios.

Información adicional
La gestión de las claves criptográficas es esencial para el uso efectivo de las técnicas criptográficas.
Los dos tipos de técnicas criptográficas son:

a. técnicas de claves secretas, donde dos o más partes comparten la misma clave y esta clave es utilizada tanto para codificar como descodificar la información, esta clave debiera mantenerse en secreto ya que cualquiera que tenga acceso a la clave puede decodificar toda la información codificada con esa clave o puede introducir información no-autorizada utilizando la clave:
b. técnicas de claves públicas, donde cada usuario tiene un par de claves, una clave pública (que puede ser revelada a cualquiera) y una clave privada (que se tiene que mantener en secreto); se pueden utilizar las técnicas de claves públicas para la codificación y para producir firmas digitales.

Existe la amenaza de la falsificación de la firma digital, reemplazándola con la clave pública de un usuario. El problema es tratado mediante el uso de un certificado de clave pública. Las técnicas criptográficas también se pueden utilizar para proteger las claves criptográficas.
Tal vez se necesite considerar procedimientos para el manejo legal del acceso a las claves criptográficas; por ejemplo, tal vez se necesite la información codificada esté disponible en una forma descodificada como evidencia en un caso en la corte.

Seguridad de los archivos del sistema
Objetivo: Garantizar la seguridad de los archivos del sistema. Se debiera controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI y las actividades de soporte se debieran realizar de una manera segura.

Control del software operacional
Control

Se debieran establecer procedimientos para el control de la instalación del software en los sistemas operacionales.

Implementación

Para minimizar el riesgo de corrupción de los sistemas operacionales, se debieran considerar los siguientes lineamientos para controlar los cambios:

a. la actualización del software operacional, aplicaciones y bibliotecas de programas sólo debiera ser realizada por administradores capacitados con la apropiada autorización gerencial;
b. los sistemas operacionales sólo debieran mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores;
c. el software de las aplicaciones y el sistema de operación sólo se debiera implementar después de una prueba extensa y satisfactoria; las pruebas debieran incluir pruebas de utilidad, seguridad, efectos sobre los sistemas y facilidad para el usuario; y se debieran llevar a cabo en sistemas separados; se debiera asegurar que se hayan actualizado todas las bibliotecas fuente correspondientes del programa;
d. se debiera utilizar un sistema de control de configuración para mantener el control de todo el software implementado, así como la documentación del sistema;
e. se debiera establecer una estrategia de "regreso a la situación original" (rollback) antes de implementar los cambios;
f. se debiera mantener un registro de auditoría de todas las actualizaciones a las bibliotecas del programa operacional;
g. se debieran mantener las versiones previas del software de aplicación como una medida de contingencia;
h. se debieran archivar las versiones antiguas del software, junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte durante todo el tiempo que se mantengan la data en archivo.

El software provisto por un vendedor y utilizado en el sistema operacional se debiera mantener en el nivel donde recibe soporte del proveedor. A lo largo del tiempo, los proveedores dejarán de dar soporte a las versiones más antiguas del software. La organización debiera considerar los riesgos de trabajar con software que no cuenta con soporte.

Cualquier decisión para actualizar a una versión nueva debiera tomar en cuenta los requerimientos comerciales para el cambio, y la seguridad de la versión; es decir, la introducción de la nueva funcionalidad de seguridad o el número y severidad de los problemas de seguridad que afectan esta versión. Se pueden aplicar algunos parches de software cuando ayudan a remover o reducir las debilidades de seguridad.

Sólo se debiera dar a los proveedores acceso físico o lógico para propósitos de soporte cuando sea necesario, y con aprobación de la gerencia. Se debieran monitorear las actividades del proveedor.
El software de cómputo puede constar del software y módulos suministrados externamente, el cual se debiera monitorear y controlar para evitar los cambios no-autorizados, los cuales introducen debilidades en la seguridad.

Información adicional
Los sistemas de operación sólo se debieran actualizar cuando existe el requerimiento para hacerlo, por ejemplo, si la versión actual del sistema de operación ya no soporta los requerimientos comerciales. Las actualizaciones no se realizan simplemente porque esté disponible una versión nueva del sistema de operación. Las versiones nuevas del sistema de operación pueden ser menos seguras, menos estables y menos entendibles que la versión actual.

Protección de la data del sistema
Control
La data de prueba se debiera seleccionar cuidadosamente, y se debiera proteger y controlar.

Implementación
Se debiera evitar el uso de bases de datos operacionales conteniendo información personal o cualquier otra información confidencial para propósitos de pruebas. Si la información personal o de otra manera confidencial se utiliza para propósitos de prueba, todos los detalles confidenciales debieran ser removidos o modificados más allá de todo reconocimiento antes de utilizarlos. Cuando se utiliza la data operacional para propósitos de prueba se debieran aplicar los siguientes lineamientos para protegerla:

a. procedimientos de control de acceso, los cuales se aplican a los sistemas de aplicación operacional, y también se debieran aplicar a los sistemas de aplicación de prueba;
b. debiera existir una autorización separada para cada vez que se copia información operacional en un sistema de aplicación de prueba;
c. la información operacional debiera ser borrada de los sistemas de aplicación de prueba inmediatamente después de haber completado la prueba;
d. se debiera registrar el copiado y uso de la información operacional para proporcionar un rastro de auditoría.

Información adicional
La prueba del sistema y aceptación usualmente requiere de volúmenes sustanciales de data de prueba que sea lo más cercana posible a la data operacional.

Control de acceso al código fuente del programa
Control
Se debiera restringir el acceso al código fuente del programa.

Implementación
El acceso al código fuente del programa y los ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debieran controlar estrictamente para evitar la introducción de una funcionalidad no-autorizada y para evitar cambios no-intencionados. Para el código fuente del programa, esto se puede lograr controlando el almacenaje central de dicho código, preferiblemente en las bibliotecas de fuentes del programa. Se debieran considerar los siguientes lineamientos para controlar el acceso a dichas bibliotecas de las fuentes del programa para reducir el potencial de corrupción de los programas de cómputo:

a. cuando sea posible, no se debieran mantener las bibliotecas de fuentes del programa en los sistemas operacionales;
b. el código fuente del programa y las bibliotecas de fuentes del programa debieran ser manejadas de acuerdo con los procedimientos establecidos;
c. el personal de soporte no debiera tener acceso irrestricto a las bibliotecas de fuentes del programa;
d. la actualización de las bibliotecas de fuentes del programa y los ítems asociados, y la emisión de las fuentes del programa para los programadores sólo se debieran realizar después de haber recibido la apropiada autorización;
e. los listados del programa se debieran mantener en un ambiente seguro;
f. se debiera mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa;
g. el mantenimiento y copiado de las bibliotecas fuentes del programa debiera estar sujeto a procedimientos estrictos de control de cambios.

Información adicional
El código fuente del programa es un código escrito por programadores, el cual es compilado (y vinculado) para crear ejecutables. Ciertos lenguajes de programación no distinguen formalmente entre el código fuente y los ejecutables ya que los ejecutables son creados en el momento que son activados.

Seguridad en los procesos de desarrollo y soporte
Objetivo: Mantener la seguridad del software y la información del sistema de aplicación. Se debiera controlar estrictamente los ambientes del proyecto y soporte.
Los gerentes responsables por los sistemas de aplicación también debieran ser responsables por la seguridad del ambiente del proyecto o el soporte. Ellos debieran asegurar que todos los cambios propuestos para el sistema sean revisados para chequear que no comprometan la seguridad del sistema o el ambiente de operación.

Procedimientos del control del cambio
Control
Se debiera controlar la implementación de los cambios mediante el uso de procedimientos formales para el control del cambio.

Implementación
Se debieran documentar y hacer cumplir los procedimientos formales de control del cambio para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y los cambios importantes a los sistemas existentes debieran realizarse después de un proceso formal de documentación, especificación, prueba, control de calidad e implementación manejada.
Este proceso debiera incluir una evaluación del riesgo, análisis de los impactos del cambio y la especificación de los controles de seguridad necesarios. Este proceso también debiera asegurar que los procedimientos de seguridad y control existentes no se vean comprometidos, que a los programadores de soporte sólo se les proporcione acceso a aquellas partes del sistema necesarias para su trabajo, y que se obtenga el acuerdo y la aprobación formal de cualquier cambio.
Cuando sea practicable, se debieran integrar los procedimientos de control de cambio operacional y en la aplicación. Los procedimientos de cambio debieran incluir:

a. mantener un registro de los niveles de autorización acordados;
b. asegurar que los cambios sean presentados por los usuarios autorizados;
c. revisar los procedimientos de control e integridad para asegurar que no se vean comprometidos por los cambios;
d. identificar todo el software, información, entidades de base de datos y hardware que requieran enmiendas;
e. obtener la aprobación formal para propuestas detalladas antes de comenzar el trabajo;
f. asegurar que los usuarios autorizados acepten a los cambios antes de la implementación;
g. asegurar que el conjunto de documentación del sistema esté actualizado al completar cada cambio y que la documentación antigua se archive o se elimine;
h. mantener un control de la versión para todas las actualizaciones del software;
i. mantener un rastro de auditoría para todas las solicitudes de cambio;
j. asegurar que la documentación de operación y procedimientos de usuarios sean cambiados conforme sean necesarios para seguir siendo apropiados;
k. asegurar que la implementación de los cambios se realicen en el momento adecuado y no disturbe los procesos comerciales involucrados.

Información adicional
El cambio de software puede tener impacto en el ambiente operacional.
La buena práctica incluye la prueba del software nuevo en un ambiente segregado de los ambientes de producción y desarrollo. Esto proporciona un medio para tener control sobre el software nuevo y permitir una protección adicional de la información

operacional que se utiliza para propósitos de pruebas. Esto incluye parches, paquetes de servicio y otras actualizaciones. Las actualizaciones automatizadas no se debieran utilizar en los sistemas críticos ya que algunas actualizaciones pueden causar que fallen las aplicaciones críticas.

Revisión técnica de la aplicación después de cambios en el sistema
Control
Cuando se cambian los sistemas de operación, se debieran revisar y probar las aplicaciones comerciales críticas para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad.

Implementación
Este proceso debiera abarcar:

a. revisar los procedimientos de control e integridad de la aplicación para asegurar que no se hayan visto comprometidos por los cambios en el sistema de operación:
b. asegurar que el plan y el presupuesto de soporte anual abarque las revisiones y pruebas del sistema resultantes de los cambios en el sistema de operación;
c. asegurar que la notificación de los cambios en el sistema de operación sea provista con tiempo para permitir realizar las pruebas y revisiones apropiadas antes de la implementación;

d. asegurar que se realicen los cambios apropiados en los planes de continuidad del negocio.

Se le debiera asignar a un grupo o persona específica la responsabilidad de monitorear las vulnerabilidades y los parches y arreglos que lancen los vendedores.

Restricciones sobre los cambios en los paquetes de software
Control
No se debieran fomentar modificaciones a los paquetes de software, se debieran limitar a los cambios necesarios y todos los cambios debieran ser estrictamente controlados.

Implementación
Mientras sea posible y practicable, se debieran utilizar los paquetes de software suministrados por vendedores sin modificaciones. Cuando se necesita modificar un paquete de software se debieran considerar los siguientes puntos:

a. el riesgo de comprometer los controles incorporados y los procesos de integridad;
b. si se debiera obtener el consentimiento del vendedor;
c. la posibilidad de obtener del vendedor los cambios requeridos como actualizaciones del programa estándar;

d. el impacto de si como resultado de los cambios, la organización se hace responsable del mantenimiento futuro del software.

Si son necesarios cambios, se debiera mantener el software original y se debieran aplicar los cambios en una copia claramente identificada. Se debiera implementar un proceso de gestión de actualizaciones del software para asegurar que la mayoría de los parches aprobados hasta – la – fecha y las actualizaciones de la aplicación se instalen para todo software autorizado. Todos los cambios debieran ser completamente probados y documentados, de manera que puedan ser re-aplicados, si fuese necesario, a las futuras actualizaciones del software. Si fuese requerido, las modificaciones debieran probadas y validadas por un organismo de evaluación independiente.

Filtración de información

Control

Se debieran evitar las oportunidades para la filtración de información.

Implementación

Se debieran considerar los siguientes puntos para limitar la filtración de la información; por ejemplo, a través del uso y explotación de los canales encubiertos (covert channels):

a. escanear el flujo de salida de los medios y las comunicaciones en busca de información escondida;
b. enmascarar y modular la conducta del sistema y las comunicaciones para reducir la probabilidad de que una tercera persona pueda deducir la información a partir de dicha conducta;
c. hacer uso de los sistemas y el software considerados de la más alta integridad; por ejemplo, utilizando productos evaluados;
d. monitoreo regular de las actividades del personal y del sistema, cuando sea permitido bajo la legislación o regulación existente;
e. monitorear la utilización del recurso en los sistemas de cómputo.

Información adicional

Los Canales Encubiertos son caminos que no están destinadas a transportar flujos de información, pero que de cualquier manera pueden existir en un sistema o red. Por ejemplo, en el manipuleo de bits se pueden utilizar paquetes de protocolo de las comunicaciones como un método escondido de señalización. Por su naturaleza, es muy difícil, sino imposible, evitar la existencia de todos los canales encubiertos posibles. Sin embargo, la explotación de dichos canales casi siempre las realiza un código Troyano. Por lo tanto, tomar medidas para protegerse contra códigos Troyanos reduce el riesgo de la explotación de los canales encubiertos.

El evitar el acceso no-autorizado a la red, así como las políticas y procedimientos para no fomentar el mal uso de los servicios de información por parte del personal ayudarán a protegerse de los canales encubiertos.

Desarrollo de software abastecido externamente
Control
El desarrollo del software abastecido externamente debiera ser supervisado y monitoreado por la organización.

Implementación
Cuando el software es abastecido externamente, se debieran considerar los siguientes puntos:

a. contratos de licencias, propiedad de códigos, derechos de propiedad intelectual ;
b. certificación de la calidad y exactitud del trabajo llevado a cabo;
c. contratos de depósito en custodia en el evento de la falla de una tercera persona;
d. derechos de acceso para a auditoría de la calidad y seguridad del trabajo realizado;
e. requerimientos contractuales para la funcionalidad de calidad y seguridad del código;
f. prueba antes de la instalación para detectar códigos maliciosos y Troyanos.

Gestión de la Vulnerabilidad Técnica
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas. Se debiera implementar una gestión de la vulnerabilidad técnica de una manera efectiva, sistemática y respetable, tomando mediciones para confirmar su efectividad. Estas consideraciones debieran incluir a los sistemas de operación, y cualquier otra aplicación en uso.

Control de las vulnerabilidades técnicas
Control
Se debiera obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, la exposición de la organización a dichas vulnerabilidades evaluadas, y las medidas apropiadas tomadas para tratar los riesgos asociados.

Implementación
Un inventario actual y completo de los activos es un prerrequisito para la gestión efectiva de la vulnerabilidad técnica. La información específica necesaria para apoyar la gestión de la vulnerabilidad técnica incluye al vendedor del software, números de la versión, estado actual del empleo (por ejemplo, cuál software está instalado en cuál sistema), y la(s) persona(s) dentro de la organización responsable(s) del software. Se debiera tomar la acción apropiada y oportuna en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se debiera seguir el siguiente lineamiento para establecer un proceso de gestión efectivo para las vulnerabilidades técnicas:

a. la organización debiera definir y establecer los roles y responsabilidades asociadas con la gestión de la vulnerabilidad técnica; incluyendo el monitoreo de

la vulnerabilidad, evaluación del riesgo de la vulnerabilidad, monitoreo de activos y cualquier responsabilidad de coordinación requerida;

b. se debieran identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener la conciencia sobre ellas para el software y otras tecnologías; estos recursos de información debieran actualizarse en base a los cambios en el inventario, o cuando se encuentran recursos nuevo o útiles;
c. se debiera definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;
d. una vez que se identifica la vulnerabilidad técnica potencial, la organización debiera identificar los riesgos asociados y las acciones a tomarse; dicha acción podría involucrar el parchado de los sistemas vulnerables y/o la aplicación de otros controles;
e. dependiendo de la urgencia con que se necesita tratar la vulnerabilidad técnica, la acción a tomarse debiera realizarse de acuerdo a los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información;
f. si es posible el parche, se debieran evaluar los riesgos asociados con instalar el parche (los riesgos impuestos por la vulnerabilidad se debieran comparar con el riesgo de instalar el parche);
g. los parches de debieran probar y evaluar antes de instalarlos para asegurar que sean efectivos y no resulten efectos secundarios que no se puedan tolerar; si el parche no está disponible, se pueden considerar otros controles:
    - desconectar los servicios o capacidades relacionadas con la vulnerabilidad;
    - adaptar o agregar controles de acceso; por ejemplo, firewalls en los límites de la red;
    - mayor monitoreo para detectar o evitar ataques reales;
    - elevar la conciencia acerca de la vulnerabilidad;
    - mantener un registro de auditoría de todos los procedimientos realizados;
    - el proceso de gestión de vulnerabilidad técnica debiera ser monitoreado y evaluado regularmente para asegurar su efectividad y eficacia;
    - se debieran tratar primero los sistemas en alto riesgo.

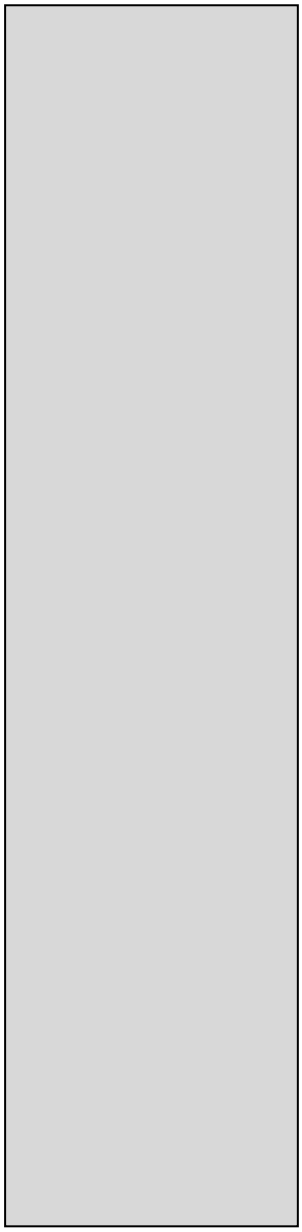
Información adicional

El correcto funcionamiento del proceso de gestión de la vulnerabilidad técnica de la organización es crítico para muchas organizaciones y por lo tanto, debiera ser monitoreado regularmente. Un inventario exacto es esencial para asegurar que se identifiquen las vulnerabilidades técnicas potencialmente relevantes.

La gestión de la vulnerabilidad técnica puede ser vista como una sub-función de la gestión de cambios y como tal pueden beneficiarse de los procesos y procedimientos de la gestión del cambio.

Con frecuencia los vendedores se ven presionados a lanzar parches lo más pronto posible. Por lo tanto, un parche puede no tratar adecuadamente el problema y puede tener efectos secundarios negativos. También, en algunos casos, no es fácil desinstalar un parche una vez que este ha sido aplicado.

Si no es posible una prueba adecuada del parche; por ejemplo, debido a los costos o falta de recursos; se puede considerar una demora en el parchado para evaluar los riesgos asociados, basados en la experiencia reportada por otros usuarios.



CAPÍTULO 6
CONCLUSIONES Y RECOMENDACIONES

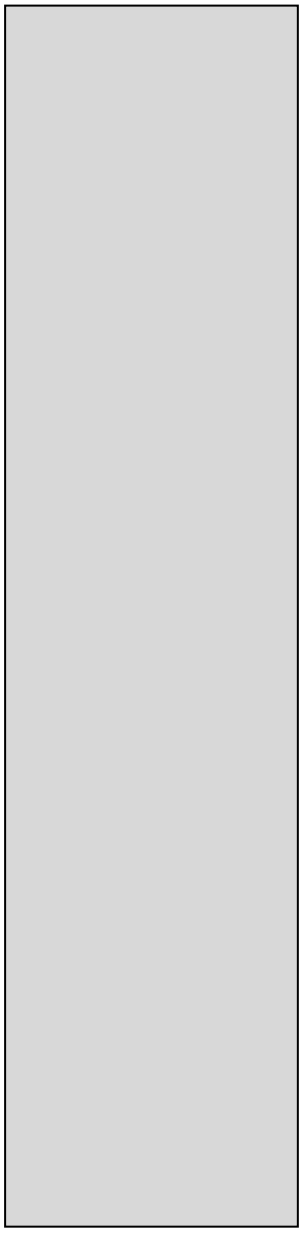
6. CONCLUSIONES Y RECOMENDACIONES

En la actualidad existen muchos riesgos y amenazas que perjudican a la información, sobre todo para aquellas empresa que desarrollan y ofrecen servicios de soporte informático a empresas medianas, grandes y corporaciones, cuyo contenido procesado es de gran valía; su modificación intencional, fortuita, sustracción por parte de la competencia desleal o destrucción supone la posible caída de la empresa, con consecuencias dentro del mercado y la sociedad en general; para evitar tales consecuencias, la implementación de estrategias, controles y procedimientos que se aplicaran para mejorar la gestión de riesgo en la empresa será basado en un exhaustivo análisis en las áreas donde la información de los clientes esté vulnerable a cualquier tipo de amenaza, sea de error fortuito o ataque premeditado.

La mayoría de las empresas manejan un gran volumen de datos de sus respectivos clientes y servicios, los cuales son indispensables para el desarrollo de la empresa en el mercado. Las estrategias que se implementaren deberán cumplir con todas las expectativas que requiere la empresa para mejorar la gestión de la información, de esta manera se establece confianza a los clientes, socios estratégicos y de la sociedad en general para garantizar calidad y confidencialidad comercial.

La prioridad que posee el área de seguridad en las tecnologías de información, se afirma en que las empresas están en la obligación, incluso de aspecto legal, de certificarse y mantener las mejores prácticas ofrecidas en las Normas Internacionales, estipuladas en la ISO 27000, ISO 27001 y la ISO 27002, cuyos estándares permitirán, después de su correcta y verificada implementación y puesta en marcha de controles minuciosos y continuos, que la empresa desarrolladora obtenga un agregado de confianza y solidez, después de su experiencia y calidad en los servicios, en la parte de la estricta confidencialidad de sus modelados de negocio. De esta manera, además de los beneficios antes descritos, se permite que exista una sana y justa competitividad entre empresas que ofrecen soporte de software.

Por ello, es indispensable que la empresa esté provista, dentro del contexto de los activos que intervienen en el presente domino detallado, de software debidamente legalizado, con sus respectivas licencias, y que en el caso de software de código libre, la Empresa observe y haga cumplir con los términos de GPL/GNU, para que el desarrollo de software mediante código libre, también esté dentro de los parámetros internacionales.



ANEXOS

7. ANEXOS

7.1. INVENTARIO DETALLADO DE LOS ACTIVOS DE DATOS

[DAT] DATOS O INFORMACION			
Código:	**CLS_DT_0001**	Nombre:	**DATOS DE ENTRADA**
Descripción:	**Datos que van a ser procesados por la aplicación o mejora a desarrollar**		
Responsable:	**Gerente de Proyectos**		
Tipo:	**[com]**		

VALORACIÓN		
Dimensión	Valor	Justificación
[I]	**8**	**[lbl]**
[C]	**9**	**[iio] [lro] [lbl]**
[D]	**9**	**[iio] [lro] [lbl]**
[A_D]	**8**	**[lbl]**
[T_D]	**8**	**[lbl]**

Dependencias de activos inferiores	
Activo:	Grado:
¿Por qué?	

[DAT] DATOS O INFORMACION			
Código:	**CLS_DT_0002**	Nombre:	**DOCUMENTO IMPRESO DE ENTRADA**
Descripción:	**Documento impreso que contiene datos de ingreso al sistema**		
Responsable:	**Gerente de Proyectos**		
Tipo:	**[com]**		

VALORACIÓN		
Dimensión	Valor	Justificación
[I]	**8**	**[lbl]**
[C]	**9**	**[iio] [lro] [lbl]**
[D]	**9**	**[iio] [lro] [lbl]**
[A_SW]	**8**	**[lbl]**
[T_SW]	**8**	**[lbl]**

Dependencias de activos inferiores	
Activo:	Grado:
¿Por qué?	

[DAT] DATOS O INFORMACION			
Código:	**CLS_DT_0003**	Nombre:	**PROCESAMIENTO INTERNO DEL SISTEMA**
Descripción:	**Operaciones a realizarse con los datos en el sistema desarrollado**		
Responsable:	**Gerente de Proyectos**		
Tipo:	**[source]**		

VALORACIÓN		
Dimensión	Valor	Justificación
[I]	**8**	**[lbl]**
[C]	**9**	**[iio] [lro] [lbl]**
[D]	**9**	**[iio] [lro] [lbl]**
[A_SW]	**8**	**[lbl]**
[T_SW]	**8**	**[lbl]**

Dependencias de activos inferiores	
Activo:	Grado:
¿Por qué?	

[DAT] DATOS O INFORMACION			
Código:	**CLS_DT_0004**	Nombre:	**MENSAJE DEL SISTEMA**
Descripción:	**Estructura de datos y operaciones a ser enviado entre elementos del sistema**		
Responsable:	**Gerente de Proyectos**		
Tipo:	**[source]**		

VALORACIÓN		
Dimensión	Valor	Justificación
[I]	**8**	**[lbl]**
[C]	**9**	**[iio] [lro] [lbl]**
[D]	**9**	**[iio] [lro] [lbl]**
[A_SW]	**8**	**[lbl]**
[T_SW]	**8**	**[lbl]**

Dependencias de activos inferiores	
Activo:	Grado:
¿Por qué?	

[DAT] DATOS O INFORMACION			
Código:	**CLS_DT_0005**	Nombre:	**CLAVES DEL SISTEMA**
Descripción:	**Datos de autenticación de los usuarios del sistema desarrollado**		
Responsable:	**Gerente de Proyectos**		
Tipo:	**[com]**		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**8**	**[lbl]**	
[C]	**9**	**[iio] [lro] [lbl]**	
[D]	**9**	**[iio] [lro] [lbl]**	
[A_SW]	**8**	**[lbl]**	
[T_SW]	**8**	**[lbl]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[DAT] DATOS O INFORMACION			
Código:	**CLS_DT_0006**	Nombre:	**CÓDIGO FUENTE**
Descripción:	**Requerimientos, diseño y especificaciones en archivos digitales o documentos impresos sobre el sistema desarrollado**		
Responsable:	**Gerente de Proyectos**		
Tipo:	**[source]**		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**8**	**[lbl]**	
[C]	**9**	**[iio] [lro] [lbl]**	
[D]	**9**	**[iio] [lro] [lbl]**	
[A_SW]	**8**	**[lbl]**	
[T_SW]	**8**	**[lbl]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[DAT] DATOS O INFORMACION			
Código:	**CLS_DT_0007**	Nombre:	**PROGRAMAS DEL SISTEMA**
Descripción:	**Datos que se almacena de forma primaria (RAM) o secundaria (discos)**		
Responsable:	**Gerente de Proyectos**		
Tipo:	**[exe]**		

VALORACIÓN		
Dimensión	Valor	Justificación
[I]	**8**	**[lbl]**
[C]	**9**	**[iio] [lro] [lbl]**
[D]	**9**	**[iio] [lro] [lbl]**
[A_SW]	**8**	**[lbl]**
[T_SW]	**8**	**[lbl]**

Dependencias de activos inferiores	
Activo:	Grado:
¿Por qué?	

[DAT] DATOS O INFORMACION			
Código:	**CLS_DT_0008**	Nombre:	**DATOS DE PRUEBA**
Descripción:	**Datos a crearse para fines de prueba en el sistema desarrollado**		
Responsable:	**Gerente de Proyectos**		
Tipo:	**[test]**		

VALORACIÓN		
Dimensión	Valor	Justificación
[I]	**8**	**[lbl]**
[C]	**9**	**[iio] [lro] [lbl]**
[D]	**9**	**[iio] [lro] [lbl]**
[A_SW]	**8**	**[lbl]**
[T_SW]	**8**	**[lbl]**

Dependencias de activos inferiores	
Activo:	Grado:
¿Por qué?	

7.2. INVENTARIO DETALLADO DE LOS ACTIVOS DE SOFTWARE

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0001**	Nombre:	**MICROSOFT WINDOWS XP SP2**
Descripción:	**Sistema operativo de disco de la computadora anfitrión** **Es Licenciado**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [os]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**7**	**[adm] [da] [olm]**	
[C]	**7**	**[cei] [iio] [lro] [lbl]**	
[D]	**6**	**[pi2] [po]**	
[A_D]	**7**	**[lro] [cei]**	
[T_D]	**5**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0002**	Nombre:	**ADOBE READER V. 9.4.4 ESPAÑOL**
Descripción:	**Aplicativo que permite solo leer archivos digitales PDF** **Licencia gratuita**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [office]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0003**	Nombre:	**APACHE TOMCAT V. 5.0**
Descripción:	**Aplicación de implementación de código abierto de las tecnologías de Java Servet y de JSP Licencia gratuita**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]**		
	[www]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:		Grado:	
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0004**	Nombre:	**AVG INTERNET SECURITY 2011**
Descripción:	**Solución antivirus, de licencia gratuita**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]**		
	[av]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:		Grado:	
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0005**	Nombre:	**BEYOND COMPARE V. 3.2.3**
Descripción:	**Permite comparar archivos y carpetas en sistemas operativos Windows y Linux, permite ver cambios en los códigos de los archivos, y los concilia Es licenciado, con periodo de prueba gratuito**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [office]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0006**	Nombre:	**EDIT PLUS V. 3**
Descripción:	**Editor de texto, archivos PHP, HTML, JAVA y es visor HEX para Windows. Es Licenciado**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [office]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0007**	Nombre:	**WINDOWS INTERNET EXPLORER 7**
Descripción:	**Navegador web** **Gratuito para usuarios de Windows**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [browser]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0008**	Nombre:	**FILEZILLA CLIENT V. 3.2.1**
Descripción:	**Solución gratuita de protocolo de transferencia de archivos (FTP)** **Es gratuito bajo términos de GNU GLP**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [file_client]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0009**	Nombre:	**MICROSOFT OUTLOOK 2007**
Descripción:	**Cliente de correo electrónico** **Es licenciado**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [email_client]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0010**	Nombre:	**MICROSOFT OFFICE ENTERPRISE 2007**
Descripción:	**Grupo de aplicaciones de oficina que combina diferentes utilizaciones de ofimática. Es totalmente licenciado**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [office]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0011**	Nombre:	**MYECLIPSE V. 5.5.1**
Descripción:	**Entorno de programación, basado en Java** **Gratuito**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]**		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:		Grado:	
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0012**	Nombre:	**ORACLE DB 10G EXPRESS EDITION**
Descripción:	**Sistema administrador de Base de Datos** **Es licenciado**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [dbms]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:		Grado:	
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0013**	Nombre:	**ORACLE VIRTUAL BOX**
Descripción:	**Emulador y virtualizador de sistemas operativos** **Es gratuito**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]** [os]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0014**	Nombre:	**PL/SQL DEVELOPER**
Descripción:	**Entorno de desarrollo orientado a lenguaje PL/SQL** **Licencia de usuario ilimitada**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]**		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0015**	Nombre:	**VMWARE PLAYER**
Descripción:	**Emula y virtualiza sistemas operativos**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]**		
	[os]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

[SW] APLICACIONES (SOFTWARE)			
Código:	**CLS_SW_0016**	Nombre:	**SPARK V. 2.5.8**
Descripción:	**Permite comunicación entre terminales de una red local Gratuito**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[std]**		
	[ts]		
VALORACIÓN			
Dimensión	Valor	Justificación	
[I]	**5**	**[adm] [da] [olm]**	
[C]	**5**	**[cei] [iio] [lro] [lbl]**	
[D]	**4**	**[pi2] [po]**	
[A_SW]	**5**	**[lro] [cei]**	
[T_SW]	**3**	**[lro] [cei]**	
Dependencias de activos inferiores			
Activo:			Grado:
¿Por qué?			

7.3. INVENTARIO DETALLADO DE LOS ACTIVOS DE SERVICIO

[S] SERVICIOS			
Código:	**CLS_S_0001**	Nombre:	**DESARROLLO DE SOFTWARE A LA MEDIDA**
Descripción:	**Servicio que presta la empresa a sus clientes a fin de implementar soluciones que satisfagan sus necesidades, y contribuir a su desarrollo continuo**		
Responsable:	**Gerente de Operaciones**		
Tipo:	**[ext]**		

VALORACIÓN		
Dimensión	Valor	Justificación
[I]	**9**	**[adm] [da] [olm] [cei.e]**
[C]	**9**	**[cei.a] [cei.e] [lg.a] [lbl]**
[D]	**9**	**[adm] [cei.b] [cei.c]**
[A_S]	**8**	**[crm] [lbl]**
[T_D]	**7**	**[adm] [olm]**

Dependencias de activos inferiores	
Activo:	Grado:
¿Por qué?	

7.4. VALORIZACIÓN TABULADA DE LAS AMENAZAS SOBRE LOS ACTIVOS

Activo	Amenaza	Dimensión	Degradación	Frecuencia	Impacto
CLS_S_0001	[E.1] Errores de los usuarios	[D] disponibilidad	75	100	87,5
		[I] integridad	75	100	87,5
	[E.2] Errores del administrador	[D] disponibilidad	75	10	42,5
		[I] integridad	75	10	42,5
		[C] confidencialidad	75	10	42,5
		[A_S] autenticidad del servicio	75	10	42,5
		[T_S] trazabilidad del servicio	50	10	30
	[E.3] Errores de monitorización (log)	[T_S] trazabilidad del servicio	75	10	42,5
	[E.4] Errores de configuración	[D] disponibilidad	50	100	75
		[I] integridad	75	100	87,5
		[C] confidencialidad	75	100	87,5
		[A_S] autenticidad del servicio	75	100	87,5
		[T_S] trazabilidad del servicio	75	100	87,5
	[E.9] Errores de [re-]encaminamiento	[I] integridad	75	100	87,5
		[C] confidencialidad	75	100	87,5
		[A_S] autenticidad del servicio	75	100	87,5
		[T_S] trazabilidad del servicio	75	100	87,5
	[E.10] Errores de secuencia	[I] integridad	50	100	75
	[E.24] Caída del sistema por agotamiento de recursos	[D] disponibilidad	75	100	87,5
CLS_DT_0001	[E.1] Errores de los usuarios	[D] disponibilidad	50	100	75
		[I] integridad	50	100	75
	[E.2] Errores del administrador	[D] disponibilidad	75	10	42,5
		[I] integridad	75	10	42,5
		[C] confidencialidad	75	10	42,5
		[A_D] autenticidad de los datos	75	10	42,5

		[T_D] trazabilidad de los datos	75	10	42,5						
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	25	10	17,5						
	[E.4] Errores de configuración	[D] disponibilidad	33	1	17						
		[I] integridad	33	1	17						
		[C] confidencialidad	33	1	17						
		[A_D] autenticidad de los datos	33	1	17						
		[T_D] trazabilidad de los datos	33	1	17						
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5						
	[E.15] Alteración de la información	[I] integridad	50	10	30						
	[E.16] Introducción de información incorrecta	[I] integridad	50	10	30						
	[E.17] Degradación de la información	[I] integridad	33	10	21,5						
	[E.18] Destrucción de información	[D] disponibilidad	33	10	21,5						
	[E.19] Divulgación de información	[C] confidencialidad	33	10	21,5						
CLS_DT_0002	[E.1] Errores de los usuarios	[I] integridad	50	100	75						
		[D] disponibilidad	50	100	75						
	[E.2] Errores del administrador	[D] disponibilidad	75	10	42,5						
		[I] integridad	75	10	42,5						
		[C] confidencialidad	75	10	42,5						
		[A_D] autenticidad de los datos	75	10	42,5						
		[T_D] trazabilidad de los datos	75	10	42,5						
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	25	10	17,5						
	[E.4] Errores de configuración	[D] disponibilidad	33	1	17						
		[I] integridad	33	1	17						
		[C] confidencialidad	33	1	17						
		[A_D] autenticidad de los datos	33	1	17						
		[T_D] trazabilidad de los datos	33	1	17						
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5						

	[E.15] Alteración de la información	[I] integridad	50	10	30
	[E.16] Introducción de información incorrecta	[I] integridad	50	10	30
	[E.17] Degradación de la información	[I] integridad	33	10	21,5
	[E.18] Destrucción de información	[D] disponibilidad	33	10	21,5
	[E.19] Divulgación de información	[C] confidencialidad	33	10	21,5
CLS_DT_0003	[E.1] Errores de los usuarios	[I] integridad	50	100	75
		[D] disponibilidad	50	100	75
	[E.2] Errores del administrador	[D] disponibilidad	75	10	42,5
		[I] integridad	75	10	42,5
		[C] confidencialidad	75	10	42,5
		[A_D] autenticidad de los datos	75	10	42,5
		[T_D] trazabilidad de los datos	75	10	42,5
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	25	10	17,5
	[E.4] Errores de configuración	[D] disponibilidad	33	1	17
		[I] integridad	33	1	17
		[C] confidencialidad	33	1	17
		[A_D] autenticidad de los datos	33	1	17
		[T_D] trazabilidad de los datos	33	1	17
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5
	[E.15] Alteración de la información	[I] integridad	50	10	30
	[E.16] Introducción de información incorrecta	[I] integridad	50	10	30
	[E.17] Degradación de la información	[I] integridad	33	10	21,5
	[E.18] Destrucción de información	[D] disponibilidad	33	10	21,5
	[E.19] Divulgación de información	[C] confidencialidad	33	10	21,5
CLS_DT_0004	[E.1] Errores de los usuarios	[I] integridad	50	100	75
		[D] disponibilidad	50	100	75
	[E.2] Errores del administrador	[D] disponibilidad	75	10	42,5

	[I] integridad	75	10	42,5
	[C] confidencialidad	75	10	42,5
	[A_D] autenticidad de los datos	75	10	42,5
	[T_D] trazabilidad de los datos	75	10	42,5
	[T_D] trazabilidad de los datos	25	10	17,5
	[D] disponibilidad	33	1	17
	[I] integridad	33	1	17
	[C] confidencialidad	33	1	17
	[A_D] autenticidad de los datos	33	1	17
	[T_D] trazabilidad de los datos	33	1	17
	[C] confidencialidad	33	10	21,5
	[I] integridad	50	10	30
	[I] integridad	50	10	30
	[I] integridad	33	10	21,5
	[D] disponibilidad	33	10	21,5
	[C] confidencialidad	33	10	21,5
CLS_DT_0005	[I] integridad	50	100	75
	[D] disponibilidad	50	100	75
	[D] disponibilidad	75	10	42,5
	[I] integridad	75	10	42,5
	[C] confidencialidad	75	10	42,5
	[A_D] autenticidad de los datos	75	10	42,5
	[T_D] trazabilidad de los datos	75	10	42,5
	[T_D] trazabilidad de los datos	25	10	17,5
	[D] disponibilidad	33	1	17
	[I] integridad	33	1	17
	[C] confidencialidad	33	1	17

	[E.3] Errores de monitorización (log)			
	[E.4] Errores de configuración			
	[E.14] Escapes de información			
	[E.15] Alteración de la información			
	[E.16] Introducción de información incorrecta			
	[E.17] Degradación de la información			
	[E.18] Destrucción de información			
	[E.19] Divulgación de información			
	[E.1] Errores de los usuarios			
	[E.2] Errores del administrador			
	[E.3] Errores de monitorización (log)			
	[E.4] Errores de configuración			

	[A_D] autenticidad de los datos	33	1	17			
	[T_D] trazabilidad de los datos	33	1	17			
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5		
	[E.15] Alteración de la información	[I] integridad	50	10	30		
	[E.16] Introducción de información incorrecta	[I] integridad	50	10	30		
	[E.17] Degradación de la información	[I] integridad	33	10	21,5		
	[E.18] Destrucción de información	[D] disponibilidad	33	10	21,5		
	[E.19] Divulgación de información	[C] confidencialidad	33	10	21,5		
CLS_DT_0006	[E.1] Errores de los usuarios	[I] integridad	50	100	75		
		[D] disponibilidad	50	100	75		
	[E.2] Errores del administrador	[D] disponibilidad	75	10	42,5		
		[I] integridad	75	10	42,5		
		[C] confidencialidad	75	10	42,5		
		[A_D] autenticidad de los datos	75	10	42,5		
		[T_D] trazabilidad de los datos	75	10	42,5		
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	25	10	17,5		
	[E.4] Errores de configuración	[D] disponibilidad	33	1	17		
		[I] integridad	33	1	17		
		[C] confidencialidad	33	1	17		
		[A_D] autenticidad de los datos	33	1	17		
		[T_D] trazabilidad de los datos	33	1	17		
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5		
	[E.15] Alteración de la información	[I] integridad	50	10	30		
	[E.16] Introducción de información incorrecta	[I] integridad	50	10	30		
	[E.17] Degradación de la información	[I] integridad	33	10	21,5		
	[E.18] Destrucción de información	[D] disponibilidad	33	10	21,5		
	[E.19] Divulgación de información	[C] confidencialidad	33	10	21,5		

CLS_DT_0007	[E.1] Errores de los usuarios	[I] integridad	50	100	75		
		[D] disponibilidad	50	100	75		
	[E.2] Errores del administrador	[D] disponibilidad	75	10	42,5		
		[I] integridad	75	10	42,5		
		[C] confidencialidad	75	10	42,5		
		[A_D] autenticidad de los datos	75	10	42,5		
		[T_D] trazabilidad de los datos	75	10	42,5		
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	25	10	17,5		
	[E.4] Errores de configuración	[D] disponibilidad	33	1	17		
		[I] integridad	33	1	17		
		[C] confidencialidad	33	1	17		
		[A_D] autenticidad de los datos	33	1	17		
		[T_D] trazabilidad de los datos	33	1	17		
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5		
	[E.15] Alteración de la información	[I] integridad	50	10	30		
	[E.16] Introducción de información incorrecta	[I] integridad	50	10	30		
	[E.17] Degradación de la información	[I] integridad	33	10	21,5		
	[E.18] Destrucción de información	[D] disponibilidad	33	10	21,5		
	[E.19] Divulgación de información	[C] confidencialidad	33	10	21,5		
CLS_DT_0008	[E.1] Errores de los usuarios	[I] integridad	50	100	75		
		[D] disponibilidad	50	100	75		
	[E.2] Errores del administrador	[D] disponibilidad	75	10	42,5		
		[I] integridad	75	10	42,5		
		[C] confidencialidad	75	10	42,5		
		[A_D] autenticidad de los datos	75	10	42,5		
		[T_D] trazabilidad de los datos	75	10	42,5		
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	25	10	17,5		

	[E.4] Errores de configuración	[D] disponibilidad	33	1	17		
		[I] integridad	33	1	17		
		[C] confidencialidad	33	1	17		
		[A_D] autenticidad de los datos	33	1	17		
		[T_D] trazabilidad de los datos	33	1	17		
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5		
	[E.15] Alteración de la información	[I] integridad	50	10	30		
	[E.16] Introducción de información incorrecta	[I] integridad	50	10	30		
	[E.17] Degradación de la información	[I] integridad	33	10	21,5		
	[E.18] Destrucción de información	[D] disponibilidad	33	10	21,5		
	[E.19] Divulgación de información	[C] confidencialidad	33	10	21,5		
CLS_SW_0001	[E.1] Errores de los usuarios	[I] integridad	33	100	66,5		
		[D] disponibilidad	33	100	66,5		
	[E.2] Errores del administrador	[D] disponibilidad	50	10	30		
		[I] integridad	50	10	30		
		[C] confidencialidad	50	10	30		
		[A_D] autenticidad de los datos	50	10	30		
		[T_D] trazabilidad de los datos	50	10	30		
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	25	10	17,5		
	[E.4] Errores de configuración	[D] disponibilidad	33	1	17		
		[I] integridad	33	1	17		
		[C] confidencialidad	33	1	17		
		[A_D] autenticidad de los datos	33	1	17		
		[T_D] trazabilidad de los datos	33	1	17		
	[E.8] Difusión de software dañino	[D] disponibilidad	50	10	30		
		[I] integridad	50	10	30		
		[C] confidencialidad	33	10	21,5		

	[A_D] autenticidad de los datos	50	10	30		
	[T_D] trazabilidad de los datos	50	10	30		
[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	50	10	30		
	[I] integridad	50	10	30		
[E.10] Errores de secuencia	[I] integridad	50	10	30		
[E.14] Escapes de información	[C] confidencialidad	50	10	30		
[E.20] Vulnerabilidades de los programas (software)	[I] integridad	50	10	30		
	[D] disponibilidad	25	10	17,5		
	[C] confidencialidad	50	10	30		
[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	50	10	30		
	[D] disponibilidad	25	10	17,5		
CLS_SW_0002 [E.1] Errores de los usuarios	[I] integridad	25	100	62,5		
	[D] disponibilidad	25	100	62,5		
[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5		
	[I] integridad	33	10	21,5		
	[C] confidencialidad	33	10	21,5		
	[A_D] autenticidad de los datos	33	10	21,5		
	[T_D] trazabilidad de los datos	33	10	21,5		
[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11		
[E.4] Errores de configuración	[D] disponibilidad	25	1	13		
	[I] integridad	25	1	13		
	[C] confidencialidad	25	1	13		
	[A_D] autenticidad de los datos	25	1	13		
	[T_D] trazabilidad de los datos	25	1	13		
[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5		
	[I] integridad	33	10	21,5		

	[C] confidencialidad	25	10	17,5
	[A_D] autenticidad de los datos	33	10	21,5
	[T_D] trazabilidad de los datos	33	10	21,5
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5
		[I] integridad	33	10	21,5
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
		[C] confidencialidad	33	10	21,5
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
CLS_SW_0003	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5
		[D] disponibilidad	25	100	62,5
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	33	10	21,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11
	[E.4] Errores de configuración	[D] disponibilidad	25	1	13
		[I] integridad	25	1	13
		[C] confidencialidad	25	1	13
		[A_D] autenticidad de los datos	25	1	13
		[T_D] trazabilidad de los datos	25	1	13
	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5

	[I] integridad	33	10	21,5
	[C] confidencialidad	25	10	17,5
	[A_D] autenticidad de los datos	33	10	21,5
	[T_D] trazabilidad de los datos	33	10	21,5
	[E.9] Errores de [re-]encaminamiento	33	10	21,5
	[I] integridad	33	10	21,5
	[I] integridad	33	10	21,5
	[C] confidencialidad	33	10	21,5
	[I] integridad	33	10	21,5
	[D] disponibilidad	12	10	11
	[C] confidencialidad	33	10	21,5
	[I] integridad	33	10	21,5
	[D] disponibilidad	12	10	11
CLS_SW_0004	[E.1] Errores de los usuarios	25	100	62,5
	[D] disponibilidad	25	100	62,5
	[E.2] Errores del administrador	33	10	21,5
	[I] integridad	33	10	21,5
	[C] confidencialidad	33	10	21,5
	[A_D] autenticidad de los datos	33	10	21,5
	[T_D] trazabilidad de los datos	33	10	21,5
	[T_D] trazabilidad de los datos	12	10	11
	[E.3] Errores de monitorización (log)	25	1	13
	[E.4] Errores de configuración	25	1	13
	[I] integridad	25	1	13
	[C] confidencialidad	25	1	13
	[A_D] autenticidad de los datos	25	1	13
	[T_D] trazabilidad de los datos	25	1	13

	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	25	10	17,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5
		[I] integridad	33	10	21,5
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
		[C] confidencialidad	33	10	21,5
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
CLS_SW_0005	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5
		[D] disponibilidad	25	100	62,5
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	33	10	21,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11
	[E.4] Errores de configuración	[D] disponibilidad	25	1	13
		[I] integridad	25	1	13
		[C] confidencialidad	25	1	13
		[A_D] autenticidad de los datos	25	1	13

	[T_D] trazabilidad de los datos	25	1	13
	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	25	10	17,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5
		[I] integridad	33	10	21,5
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
		[C] confidencialidad	33	10	21,5
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
CLS_SW_0006	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5
		[D] disponibilidad	25	100	62,5
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	33	10	21,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11
	[E.4] Errores de configuración	[D] disponibilidad	25	1	13
		[I] integridad	25	1	13
		[C] confidencialidad	25	1	13

		[A_D] autenticidad de los datos	25	1	13							
		[T_D] trazabilidad de los datos	25	1	13							
	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5							
		[I] integridad	33	10	21,5							
		[C] confidencialidad	25	10	17,5							
		[A_D] autenticidad de los datos	33	10	21,5							
		[T_D] trazabilidad de los datos	33	10	21,5							
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5							
		[I] integridad	33	10	21,5							
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5							
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5							
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5							
		[D] disponibilidad	12	10	11							
		[C] confidencialidad	33	10	21,5							
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5							
		[D] disponibilidad	12	10	11							
CLS_SW_0007	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5							
		[D] disponibilidad	25	100	62,5							
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5							
		[I] integridad	33	10	21,5							
		[C] confidencialidad	33	10	21,5							
		[A_D] autenticidad de los datos	33	10	21,5							
		[T_D] trazabilidad de los datos	33	10	21,5							
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11							
	[E.4] Errores de configuración	[D] disponibilidad	25	1	13							
		[I] integridad	25	1	13							

	[C] confidencialidad	25	1	13			
	[A_D] autenticidad de los datos	25	1	13			
	[T_D] trazabilidad de los datos	25	1	13			
	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5		
		[I] integridad	33	10	21,5		
		[C] confidencialidad	25	10	17,5		
		[A_D] autenticidad de los datos	33	10	21,5		
		[T_D] trazabilidad de los datos	33	10	21,5		
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5		
		[I] integridad	33	10	21,5		
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5		
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5		
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5		
		[D] disponibilidad	12	10	11		
		[C] confidencialidad	33	10	21,5		
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5		
		[D] disponibilidad	12	10	11		
CLS_SW_0008	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5		
		[D] disponibilidad	25	100	62,5		
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5		
		[I] integridad	33	10	21,5		
		[C] confidencialidad	33	10	21,5		
		[A_D] autenticidad de los datos	33	10	21,5		
		[T_D] trazabilidad de los datos	33	10	21,5		
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11		
	[E.4] Errores de configuración	[D] disponibilidad	25	1	13		

	[I] integridad	25	1	13					
	[C] confidencialidad	25	1	13					
	[A_D] autenticidad de los datos	25	1	13					
	[T_D] trazabilidad de los datos	25	1	13					
	[D] disponibilidad	33	10	21,5					
	[I] integridad	33	10	21,5					
	[C] confidencialidad	25	10	17,5					
	[A_D] autenticidad de los datos	33	10	21,5					
	[T_D] trazabilidad de los datos	33	10	21,5					
	[C] confidencialidad	33	10	21,5					
	[I] integridad	33	10	21,5					
	[I] integridad	33	10	21,5					
	[C] confidencialidad	33	10	21,5					
	[I] integridad	33	10	21,5					
	[D] disponibilidad	12	10	11					
	[C] confidencialidad	33	10	21,5					
	[I] integridad	33	10	21,5					
	[D] disponibilidad	12	10	11					
CLS_SW_0009	[I] integridad	25	100	62,5					
	[D] disponibilidad	25	100	62,5					
	[D] disponibilidad	33	10	21,5					
	[I] integridad	33	10	21,5					
	[C] confidencialidad	33	10	21,5					
	[A_D] autenticidad de los datos	33	10	21,5					
	[T_D] trazabilidad de los datos	33	10	21,5					
	[T_D] trazabilidad de los datos	12	10	11					

	[E.4] Errores de configuración	[D] disponibilidad	25	1	13
		[I] integridad	25	1	13
		[C] confidencialidad	25	1	13
		[A_D] autenticidad de los datos	25	1	13
		[T_D] trazabilidad de los datos	25	1	13
	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	25	10	17,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5
		[I] integridad	33	10	21,5
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
		[C] confidencialidad	33	10	21,5
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
CLS_SW_0010	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5
		[D] disponibilidad	25	100	62,5
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	33	10	21,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5

	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11
	[E.4] Errores de configuración	[D] disponibilidad	25	1	13
		[I] integridad	25	1	13
		[C] confidencialidad	25	1	13
		[A_D] autenticidad de los datos	25	1	13
		[T_D] trazabilidad de los datos	25	1	13
	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	25	10	17,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5
		[I] integridad	33	10	21,5
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
		[C] confidencialidad	33	10	21,5
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
CLS_SW_0011	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5
		[D] disponibilidad	25	100	62,5
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	33	10	21,5
		[A_D] autenticidad de los datos	33	10	21,5

		[T_D] trazabilidad de los datos	33	10	21,5
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11
	[E.4] Errores de configuración	[D] disponibilidad	25	1	13
		[I] integridad	25	1	13
		[C] confidencialidad	25	1	13
		[A_D] autenticidad de los datos	25	1	13
		[T_D] trazabilidad de los datos	25	1	13
	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	25	10	17,5
		[A_D] autenticidad de los datos	33	10	21,5
		[T_D] trazabilidad de los datos	33	10	21,5
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5
		[I] integridad	33	10	21,5
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
		[C] confidencialidad	33	10	21,5
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5
		[D] disponibilidad	12	10	11
CLS_SW_0012	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5
		[D] disponibilidad	25	100	62,5
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5
		[I] integridad	33	10	21,5
		[C] confidencialidad	33	10	21,5

	[A_D] autenticidad de los datos	33	10	21,5
	[T_D] trazabilidad de los datos	33	10	21,5
[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11
[E.4] Errores de configuración	[D] disponibilidad	25	1	13
	[I] integridad	25	1	13
	[C] confidencialidad	25	1	13
	[A_D] autenticidad de los datos	25	1	13
	[T_D] trazabilidad de los datos	25	1	13
[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5
	[I] integridad	33	10	21,5
	[C] confidencialidad	25	10	17,5
	[A_D] autenticidad de los datos	33	10	21,5
	[T_D] trazabilidad de los datos	33	10	21,5
[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5
	[I] integridad	33	10	21,5
[E.10] Errores de secuencia	[I] integridad	33	10	21,5
[E.14] Escapes de información	[C] confidencialidad	33	10	21,5
[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5
	[D] disponibilidad	12	10	11
	[C] confidencialidad	33	10	21,5
[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5
	[D] disponibilidad	12	10	11
CLS_SW_0013 [E.1] Errores de los usuarios	[I] integridad	25	100	62,5
	[D] disponibilidad	25	100	62,5
[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5
	[I] integridad	33	10	21,5

	[C] confidencialidad	33	10	21,5			
	[A_D] autenticidad de los datos	33	10	21,5			
	[T_D] trazabilidad de los datos	33	10	21,5			
	[T_D] trazabilidad de los datos	12	10	11			
	[D] disponibilidad	25	1	13			
	[I] integridad	25	1	13			
	[C] confidencialidad	25	1	13			
	[A_D] autenticidad de los datos	25	1	13			
	[T_D] trazabilidad de los datos	25	1	13			
	[D] disponibilidad	33	10	21,5			
	[I] integridad	33	10	21,5			
	[C] confidencialidad	25	10	17,5			
	[A_D] autenticidad de los datos	33	10	21,5			
	[T_D] trazabilidad de los datos	33	10	21,5			
	[C] confidencialidad	33	10	21,5			
	[I] integridad	33	10	21,5			
	[I] integridad	33	10	21,5			
	[C] confidencialidad	33	10	21,5			
	[I] integridad	33	10	21,5			
	[D] disponibilidad	12	10	11			
	[C] confidencialidad	33	10	21,5			
	[I] integridad	33	10	21,5			
	[D] disponibilidad	12	10	11			
CLS_SW_0014	[I] integridad	25	100	62,5			
	[D] disponibilidad	25	100	62,5			
	[D] disponibilidad	33	10	21,5			

	[I] integridad	33	10	21,5						
	[C] confidencialidad	33	10	21,5						
	[A_D] autenticidad de los datos	33	10	21,5						
	[T_D] trazabilidad de los datos	33	10	21,5						
	[T_D] trazabilidad de los datos	12	10	11						
	[D] disponibilidad	25	1	13						
	[I] integridad	25	1	13						
	[C] confidencialidad	25	1	13						
	[A_D] autenticidad de los datos	25	1	13						
	[T_D] trazabilidad de los datos	25	1	13						
	[D] disponibilidad	33	10	21,5						
	[I] integridad	33	10	21,5						
	[C] confidencialidad	25	10	17,5						
	[A_D] autenticidad de los datos	33	10	21,5						
	[T_D] trazabilidad de los datos	33	10	21,5						
	[C] confidencialidad	33	10	21,5						
	[I] integridad	33	10	21,5						
	[I] integridad	33	10	21,5						
	[C] confidencialidad	33	10	21,5						
	[I] integridad	33	10	21,5						
	[D] disponibilidad	12	10	11						
	[C] confidencialidad	33	10	21,5						
	[I] integridad	33	10	21,5						
	[D] disponibilidad	12	10	11						
CLS_SW_0015	[I] integridad	25	100	62,5						
	[D] disponibilidad	25	100	62,5						

[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5			
	[I] integridad	33	10	21,5			
	[C] confidencialidad	33	10	21,5			
	[A_D] autenticidad de los datos	33	10	21,5			
	[T_D] trazabilidad de los datos	33	10	21,5			
[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11			
[E.4] Errores de configuración	[D] disponibilidad	25	1	13			
	[I] integridad	25	1	13			
	[C] confidencialidad	25	1	13			
	[A_D] autenticidad de los datos	25	1	13			
	[T_D] trazabilidad de los datos	25	1	13			
[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5			
	[I] integridad	33	10	21,5			
	[C] confidencialidad	25	10	17,5			
	[A_D] autenticidad de los datos	33	10	21,5			
	[T_D] trazabilidad de los datos	33	10	21,5			
[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5			
	[I] integridad	33	10	21,5			
[E.10] Errores de secuencia	[I] integridad	33	10	21,5			
[E.14] Escapes de información	[C] confidencialidad	33	10	21,5			
[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5			
	[D] disponibilidad	12	10	11			
	[C] confidencialidad	33	10	21,5			
[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5			
	[D] disponibilidad	12	10	11			
CLS_SW_0016	[E.1] Errores de los usuarios	[I] integridad	25	100	62,5		

		[D] disponibilidad	25	100	62,5					
	[E.2] Errores del administrador	[D] disponibilidad	33	10	21,5					
		[I] integridad	33	10	21,5					
		[C] confidencialidad	33	10	21,5					
		[A_D] autenticidad de los datos	33	10	21,5					
		[T_D] trazabilidad de los datos	33	10	21,5					
	[E.3] Errores de monitorización (log)	[T_D] trazabilidad de los datos	12	10	11					
	[E.4] Errores de configuración	[D] disponibilidad	25	1	13					
		[I] integridad	25	1	13					
		[C] confidencialidad	25	1	13					
		[A_D] autenticidad de los datos	25	1	13					
		[T_D] trazabilidad de los datos	25	1	13					
	[E.8] Difusión de software dañino	[D] disponibilidad	33	10	21,5					
		[I] integridad	33	10	21,5					
		[C] confidencialidad	25	10	17,5					
		[A_D] autenticidad de los datos	33	10	21,5					
		[T_D] trazabilidad de los datos	33	10	21,5					
	[E.9] Errores de [re-]encaminamiento	[C] confidencialidad	33	10	21,5					
		[I] integridad	33	10	21,5					
	[E.10] Errores de secuencia	[I] integridad	33	10	21,5					
	[E.14] Escapes de información	[C] confidencialidad	33	10	21,5					
	[E.20] Vulnerabilidades de los programas (software)	[I] integridad	33	10	21,5					
		[D] disponibilidad	12	10	11					
		[C] confidencialidad	33	10	21,5					
	[E.21] Errores de mantenimiento / actualización de programas (software)	[I] integridad	33	10	21,5					
		[D] disponibilidad	12	10	11					

7.5. CUADRO SOA DETALLADO

Leyenda (para los Controles seleccionados y sus Razones)

LR: Requerimientos legales, **CO**: Obligaciones contractuales, **BR/BP**: Requerimientos del negocio/adopción de buenas prácticas, **RRA**: resultados de la evaluación de riesgos, **TSE**: hasta cierto límite

ISO 27001:2005 Controles			Controles Actuales	Observaciones (justificación de la exclusión)	Controles Seleccionados y Razones de Selección				Comentarios (descripción general de la aplicación)
					LR	CO	BR/ BP	RRA	
Dominio	**Sección**	**Control/ Objetivos de Control**							
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	12.1	Requerimientos de Seguridad de Sistemas de Información							
	12.1.1	Análisis y Especificaciones de Requerimientos de Seguridad	SI			✓			Centro de datos no hace ningún mantenimiento o apoyo de desarrollo de software de aplicación del sistema. No obstante las mejoras en el hardware (es decir, discos adicionales, etc.) requieren una solicitud de cambio
	12.2	Procesamiento Correcto en Aplicaciones							

	12.2.1	Validación de Entrada de Datos	NO				✓	Centro de datos no hace ningún mantenimiento o apoyo de desarrollo de software de aplicación del sistema
	12.2.2	Control de Procesamiento Interno	NO				✓	Centro de datos no hace ningún mantenimiento o apoyo de desarrollo de software de aplicación del sistema
	12.2.3	Integridad del Mensaje	NO				✓	Centro de datos no hace ningún mantenimiento o apoyo de desarrollo de software de aplicación del sistema
	12.2.4	Validación de Salida de Datos	NO				✓	Centro de datos no hace ningún mantenimiento o apoyo de desarrollo de software de aplicación del sistema
	12.3	Controles Criptográficos						
	12.3.1	Directivas en el uso de controles criptográficos	NO				✓	Controles criptográficos son de aplicación específica y no con el apoyo de AGS

	12.3.2	Administración de Claves	NO					Controles criptográficos son de aplicación específica y no con el apoyo de AGS
	12.4	Seguridad de Sistemas de Archivos						
	12.4.1	Control de Software Operacional	SI				✓	Para evitar el control de cambios no autorizados
	12.4.2	Protección de datos de prueba de sistema	NO				✓	Centro de datos no hace ningún mantenimiento o apoyo de desarrollo de software de aplicación del sistema
	12.4.3	Control de acceso a librerías del programa fuente	SI				✓	El código fuente se alojó como una copia de seguridad solamente
	12.5	Seguridad en Procesos de Desarrollo y Soporte						
	12.5.1	Procedimientos de Control de Cambios	SI				✓	Cualquier cambio de centro de datos de activos requiere una solicitud de cambio

12.5.2	Revisión Técnica de aplicaciones después de cambios en el Sistema Operativo	SI				✓		No en competencia de los centros de datos, pero que informar a los dueños de las aplicaciones de los sistemas operativos, cuando se han producido cambios
12.5.3	Restricciones en cambios a paquetes de software	NO				✓		Los paquetes de software no son utilizados por AGS. (El software de aplicación controlada por el procedimiento de control de cambios)
12.5.4	Fuga de Información	SI				✓		Oportunidades para la fuga de información deben evitarse
12.5.5	Desarrollo de Software fuera de las fuentes autorizadas	NO				✓		El desarrollo de software no se hace por AGS
12.6	Técnicas en gestión de vulnerabilidades							
12.6.1	Control de vulnerabilidades técnicas	SI					✓	Vulnerabilidades técnicas deben ser gestionados