ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DESARROLLO E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICANDO EL ESTÁNDAR ISO/IEC 27002 PARA EL DEPARTAMENTO DE SISTEMAS DE UNA EMPRESA DEL SECTOR FARMACÉUTICO DE ECUADOR"

TRABAJO DE TITULACIÓN

Previo a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por

JUAN EDUARDO GUERRERO CUEVA

Guayaquil - Ecuador

2017

AGRADECIMIENTO

A Dios que me ha colmado de bendiciones, para luchar y vencer los obstáculos que se presentan a diario.

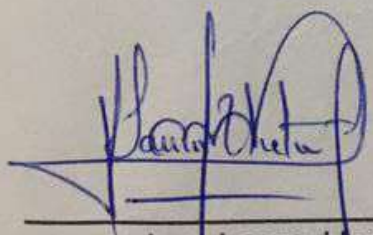
A mis familia ya que gracias a su sacrificio he podido dar un paso más e importante en mi vida.

DEDICATORIA

Para Juan Eduardo Guerrero Pérez, quien es mi fuerza para seguir adelante, y que el final de mis trabajos solo sea el inicio de los suyos.

TRIBUNAL DE GRADUACIÓN

Ing. Lenin Freire C.
DIRECTOR MSIA

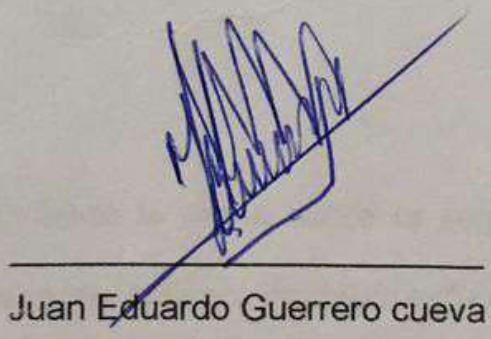


Ing. Laura Ureta A.
DIRECTOR DEL PROYECTO DE GRADUACIÓN

Ing. Juan García
MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en esta Tesis de Grado le corresponden exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL"



Juan Eduardo Guerrero cueva

RESUMEN

Esta tesis de grado tiene como objetivo general diseñar e implementar una política de seguridad basado en el estándar ISO /IEC 27002 aplicado en tres dominios.

En el primer capítulo se describe el problema inicial, en el cual se plantea una solución mediante la aplicación de normas aceptadas internacionalmente, también describe los objetivos propios de la tesis de grado.

El segundo capítulo contiene la teoría sobre la seguridad informática, los estándares y normas que se aplican, también incluye una revisión de las metodologías de análisis de gestión del riesgo para finalmente entrar en detalle en el estándar ISO/IEC 27002

El tercer capítulo define el lugar donde se quiere implementar las políticas, realizando un análisis sobre la situación actual en la que se encuentra el departamento de sistemas, con ayuda de una encuesta y de las estadísticas que se llevan como información sobre los incidentes.

En el cuarto capítulo análisis y diseño de la política, dentro del análisis se estudian los controles seleccionados en base a la norma y también se selecciona la metodología con la cual se va a realizar la medición del riesgo para finalmente concluir con el diseño de la política

En el quinto capítulo se revisa lo necesario para que la política pueda ser implementada, así como las pruebas y la difusión a los usuarios.

En el capítulo seis se realiza una evaluación posterior con el fin de verificar si las amenazas presentadas fueron mitigadas y si el riesgo residual es aceptado. Y por último se evalúa el impacto que tiene la implementación de políticas en la gestión administrativa

Finalmente, se encuentran las conclusiones y recomendaciones de la presente tesis de grado así como sus anexos.

ABREVIATURAS Y SIMBOLOGÍA

DBA	Administrador de Base de Datos
DS	Departamento de Sistemas
IEC	Comisión Electrotécnica Internacional
IP	Protocolo de Internet
ISO	Organización Internacional de Normalización
HP	Hewlett Packard
PC	Computador Personal
PDCA	las siglas se corresponden a plan-do-check-act, (planificar-hacer-verificar-actuar) también se lo conoce como círculo de Deming o espiral de mejora continua [1]
SGSI	Sistema de Gestión de Seguridad de la Información

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Con el uso acelerado y el desarrollo de los computadores en la década de los 80 y la aparición de nuevas amenazas como virus informáticos en la década de los noventas, empieza a surgir la preocupación por la seguridad de los datos así como de su integridad confidencialidad y disponibilidad. Con el pasar de los años se generaliza el uso del internet lo que trae consigo nuevas amenazas como los virus, gusanos, malware y ataques realizados por hackers.

Es por ello que nace el concepto de seguridad informática, que consiste en aplicar distintas técnicas desde normas hasta controles, con el fin de proteger el activo más importante que se tiene hoy en día en la organización, esto es la información.

Aunque no es posible eliminar el riesgo completamente, es posible reducirlos considerablemente con el uso de controles los cuales ayudan a contrarrestar las amenazas que puedan afectar la seguridad de la organización. Estos controles deben estar en constante revisión y actualización para que se mantengan al día con los cambios que se presentan en la tecnología con el paso del tiempo.

La implementación de políticas y controles es específico para cada organización, para esto es necesario analizar los controles existentes y posterior realizar un análisis de riesgos para finalmente los controles seleccionados ser presentados a la dirección y puedan ser comunicados y expuestos luego de su aprobación

Con la presente tesis de grado se busca establecer la Política de Seguridad y aplicar los controles recomendados por las norma con el fin de mitigar el riesgo que se presenta en los procesos seleccionados que maneja el departamento de sistemas.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

Antes de que existiera la norma ISO 27002 el estándar era conocido como el ISO/IEC 17799 y fue publicado en el año de 1995, para el año 2000 la organización internacional de normalización pública el estándar en su versión 2000 con el nombre de Técnicas de seguridad Código de prácticas para la gestión de la seguridad de la información. Luego en el 2005 tuvo su siguiente actualización [13].

En el año 2005 se reserva la numeración 27000 para todo lo relacionado a la seguridad de la información y en octubre de ese año se aprueba el estándar IGFSO/DIEC 17799 que luego fue llamado ISO/IEC 27002 en el año 2007

Al día de hoy ya se cuenta con la norma ISO/IEC 27002:2013 que es un estándar que proporciona controles que pueden ser utilizados dentro de la implementación de un sistema de gestión de seguridad y que pueden ser utilizadas como base para crear nuevas políticas o directrices. Los dominios que maneja la norma ISO/IEC 27002:2013 son [12]:

- POLÍTICA DE SEGURIDAD.
- ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.
- GESTIÓN DE ACTIVOS.
- SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- SEGURIDAD FÍSICA Y DEL ENTORNO.
- GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- CONTROL DE ACCESO.
- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
- GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

- GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- CUMPLIMIENTO.

La norma cuenta con 14 dominios, 35 objetivos de control y 114 controles.

1.2 DESCRIPCIÓN DEL PROBLEMA

Actualmente, el departamento de sistemas no cuenta con un esquema de seguridad informática que incluya una política de seguridad en la que se establezcan procedimientos con referencia a responsabilidades, sistemas de control accesos, uso de los recursos informáticos y demás mencionados en la norma. La Organización con el paso de los años ha tenido un crecimiento acelerado tanto en personal como en activos informáticos por lo cual, se ha considerado que existe un aumento en los riesgos.

La seguridad informática, se enfoca en entender el riesgo y como las vulnerabilidades pueden causar grandes pérdidas a la empresa, es por ello que surge la necesidad de proveer un conjunto de políticas que ayuden a mitigar este riesgo teniendo en cuenta los aspectos de la confidencialidad, integridad y disponibilidad.

El no mantener una política de seguridad, aumenta el riesgo de que ocurran pérdidas de información o paralizaciones a nivel de operaciones, ante esta situación se trabajará en los diferentes departamentos del área de sistemas que son desarrollo, infraestructura, operaciones, comunicaciones y base de datos con el objetivo de proveer políticas que ayuden a mitigar el riesgo que pueda presentarse, con el apoyo de la administración para su definición e implantación.

Dentro de los incidentes que se han presentado en los dos últimos años tenemos los siguientes:

- Errores por subida de información de prueba en ambiente de producción.
- Borrado de información por no tener escalamiento de permisos.
- Pérdida de información por falta de procedimiento de respaldo.
- Ejecución de scripts en ambientes de producción con errores.
- Accesos al sistema con usuarios que ya no se encuentran en el departamento.

- Acceso utilizando usuarios por defecto.
- Uso de claves de acceso con bajo nivel de dificultad o complejidad.
- Falta de procedimiento para el uso de dispositivos removibles.

Estos incidentes han generado en más de una ocasión reprocesos de información que implican días resolverlo entre el personal de soporte y operaciones, cuyo resultado deriva en el retraso de las actividades diarias de los miembros del departamento. En otros casos como la ejecución de pruebas en ambiente de producción ha causado fallas a nivel de inventarios y costos de productos ocasionando que los usuario no tengan la información al día y completa.

1.3 SOLUCIÓN PROPUESTA

Analizar, elaborar y diseñar, un esquema en el cual se defina una política de seguridad informática soportada en procedimientos que ayuden a garantizar la seguridad de la información basados en el estándar ISO/IEC 27002, aplicando los controles necesarios de los dominios de Aspectos organizativos de la seguridad de la información, Manejo de medios, Control de Accesos, Desarrollo y mantenimiento de software.

La ISO/IEC 27002 proporciona un conjunto de recomendaciones y de buenas prácticas en la gestión de seguridad de la información. Esta norma es de gran ayuda para quienes desean implementar sistemas de gestión de seguridad ya que se enfoca en la confidencialidad, disponibilidad e integridad de la información.

Al hacer uso de esta norma se identificaran y se evaluarán las vulnerabilidades de los activos de información, a través de una identificación, análisis y tratamiento de riesgos, por el cual se definirá y aplicarán controles u otras formas para el tratamiento de los mismos.

Para el efecto, se realizará un análisis de seguridad en el departamento, a fin de determinar el grado de madurez que se tiene en las diferentes áreas, basándonos en lo que nos indica la norma ISO/IEC 27002:2013, es decir, se hará un levantamiento de información para luego realizar un análisis de riesgos, definir los dominios de la norma que aplicaran para la política, acorde con el alcance establecido, seguido de las pruebas y plan de implementación que incluirá la capacitación y difusión de la política.

Los beneficios de un sistema de seguridad con políticas claramente concebidas bien elaboradas son inmediatos, ya que se trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Disminuir los tiempos destinados a la corrección de errores
- Disminuir los incidentes reportados, al disminuir el número de incidentes reportados se reduce la cantidad de recursos destinados a resolver incidentes lo cual se puede cuantificar en hora/recurso y su respectivo valor.
- Mejorar las relaciones laborales, ya que dejaran de existir roces entre las áreas involucradas por motivos de quien debe dar solución a los incidentes.
- Asegurar la información, se podrá realizar un control y monitoreo adecuado a la información que se maneja.
- Fortalecer en la seguridad de los accesos al sistema a nivel de claves.

1.4 OBJETIVO GENERAL

Desarrollar e implementar políticas de seguridad informática, aplicando la estándar ISO/IEC 27002:2013 para lograr niveles adecuados de integridad, confidencialidad y disponibilidad de la información en el departamento de sistema de la empresa del sector farmacéutico.

1.5 OBJETIVOS ESPECIFICOS

- Realizar un diagnóstico para conocer la situación actual relacionada con las distintas áreas dentro del departamento de sistemas
- Identificar los elementos de riesgos y fallas de seguridad informática
- Elaborar un informe de acuerdo a los hallazgos encontrados, según el estándar ISO/IEC 27002:2013
- Proponer un manual de políticas de seguridad informática para la empresa farmacéutica.
- Implementar y difundir la política y procedimientos basados en el estándar ISO/IEC 27002:2013.

1.6 ALCANCE

Desarrollar e implementar políticas de seguridad informática aplicando el estándar ISO/IEC 27002:2013 para el departamento de sistemas de una

empresa del sector farmacéutico de Ecuador basado en los dominios de Manejo de medios, Control de Accesos, Desarrollo y mantenimiento de software.

CAPÍTULO 2

MARCO TEÓRICO

2.1 SEGURIDAD INFORMÁTICA

La seguridad informática es un área de la informática que se basa en el diseño de normas, creación de procedimientos y controles para asegurar la integridad, disponibilidad y confiabilidad de la información.

Las normas, procedimientos y controles pueden estar dirigidos tanto a hardware como a software. Una vez establecidos deben ser monitoreados y

revisados periódicamente con el fin de asegurar que están cumpliendo los objetivos para los que fueron creados.

Figura 2.1 Aspectos de la Seguridad de la Información

En la figura 2.1 se presentan tres aspectos que definen si un sistema es seguro o no, confidencialidad, disponibilidad e integridad, además de que estos aspectos se consideran como el pilar fundamental de la seguridad de la información. La confidencialidad de la información, implica, que solo accedan a esta quienes tienen los accesos autorizados, integridad de la información es el concepto que nos indica que la información a la que accedemos no haya sido alterada o manipulada por personas no autorizadas y por último la disponibilidad de la información se refiere a que la información se encuentre accesible cada vez que se requiera [14].

2.2 ESTÁNDARES Y NORMAS APLICABLES

La implementación de un SGSI se explica a través de las normas IS 27000 y lo que se busca con esta implementación es proteger la información basándose en tres objetivos:

1. Confidencialidad
2. Integridad
3. Disponibilidad

Al implementar una norma ISO 27002 en la organización garantiza, que el riesgo en la seguridad de la información está siendo controlado de forma eficiente.

2.2.1 ISO / IEC 27000

A continuación se presenta un cuadro resumen con los estándares existentes de la familia ISO 27000 las mismas que se detallan con su año de publicación y una descripción sobre que parte de la seguridad de la información hacen referencia [9].

La ISO 27000 Sigue el modelo PDCA también conocido como círculo de Deming o espiral de la mejora continua [1].

Tabla 1 Familia ISO 27000

Norma	Publicación	Descripción
ISO/IEC 27003	1 de Febrero de 2010	Es una guía para el diseño e implementación con éxito de un SGSI
ISO/IEC 27004	15 de Diciembre de 2009	Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI
ISO/IEC 27005	1 de Junio de 2011	Proporciona directrices para la gestión del riesgo en la seguridad de la información.
ISO/IEC 27006	1 de diciembre de 2011	Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información
ISO/IEC 27007	14 de Noviembre de 2011	Es una guía de auditoría de un SGSI
ISO/IEC 27008	15 de Octubre de 2011	Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI
ISO/IEC 27010	20 de Octubre de 2012	Guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores
ISO/IEC 27011	15 de Diciembre de 2008	Guía de implementación y gestión de la seguridad de la información para el sector de las telecomunicaciones
ISO/IEC 27013	15 de Octubre de 2012	Guía de implementación de ISO/IEC 27001:2005 (gestión de seguridad de la información).
ISO/IEC TR 27015	23 de Noviembre de 2012	Guía de SGSI orientada a organizaciones del sector financiero y de seguros
ISO/IEC TR 27016	20 de febrero de 2014	Guía de valoración de los aspectos financieros de la seguridad de la información.

Tabla 2 Familia ISO 27000

Norma	Publicación	Descripción
ISO/IEC 27017	15 de Diciembre de 2015	Guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube
ISO/IEC TR 27019	17 de Julio de 2013	Guía para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía
ISO/IEC TR 27023	2 de Julio de 2015	Es una guía de relación entre las versiones del 2005 y 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002
ISO/IEC 27031	01 de Marzo de 2011	Guía para la adecuación de las TIC sobre la continuidad del negocio
ISO/IEC 27032	16 de Julio de 2012	Guía para la mejora del estado de la cyberseguridad
ISO/IEC 27035	17 de Agosto de 2011	Guía sobre la gestión de incidentes de seguridad en la información
ISO/IEC 27036	27 de Febrero 2014	Seguridad en entornos de servicios Cloud
ISO/IEC 27037	15 de Octubre de 2012	Guía de directrices para las actividades de identificación, recopilación, consolidación y preservación de evidencias digitales
ISO/IEC 27038	13 de Marzo de 2014	Guía para seguridad en la redacción digital
ISO/IEC 27039	11 de Febrero de 2015	Guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión
ISO/IEC 27040	5 de Enero de 2015	Guía para la seguridad en medios de almacenamiento
ISO/IEC 27041 a 27043	19 de Junio de 2015	Guía con directrices para el análisis e interpretación de las evidencias digitales
ISO 27799	12 de Junio de 2008	Guía en cuanto a la seguridad de la información sobre los datos de salud de los pacientes

Familia ISO / IEC 27000 con su descripción y fecha de publicación con mes y año[2].

2.3 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGO

El proceso de análisis de riesgos, se inicia con el inventario de activos para luego de ello identificar las amenazas a las que se encuentran expuestos así como el nivel de probabilidad de que el riesgo se materialice es así que se puede determinar el impacto que producirían tales riesgos si llegaran a ocurrir. Este análisis nos ayudara a determinar los controles con los cuales vamos a mitigar el riesgo, aceptarlo o transferirlo.

En caso de que un riesgo llegara a materializarse esta representaría pérdidas económicas en la organización así como trabajo administrativo para tratar de revertir el daño ocasionado, es ahí cuando la aplicación de los controles recomendados por las normas y metodologías que ayudan a estimar la magnitud del riesgo. Cabe recalcar que estos controles deben enfocarse en la confiabilidad, integridad y disponibilidad de la información.

El resultado del análisis de riesgo es llamado matriz de riesgo, es una matriz en la cual se manejan dos ejes que son magnitud del daño y probabilidad de que la amenaza se vuelva real [15].

Para determinar el riesgo total de una amenaza se aplica la siguiente formula:

(2.1) RT (Riesgo Total) = Probabilidad x Impacto Promedio

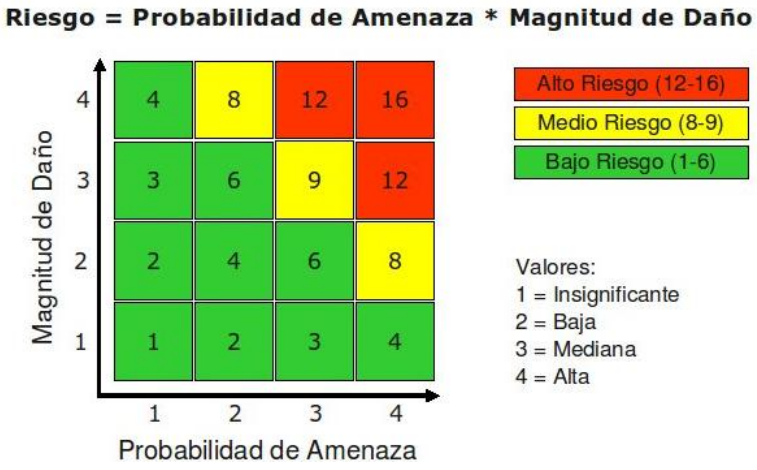


Figura 2.2 Matriz de Riesgo

Matriz de riesgo, es en la que a través de una escala de valores podemos identificar si el riesgo total al que está expuesto es alto, medio o bajo.

A partir de esta fórmula determinaremos su tratamiento y después de aplicar los controles podremos obtener el riesgo residual. Las metodologías a evaluar son:

1. Octave-Allegro

2. MAGERIT
3. ISO 27005

2.3.1 METODOLOGÍA OCTAVE ALLEGRO

Octave-allegro Diseñado para permitir una amplia evaluación de los riesgos operacionales de la organización con el objetivo de entregar resultados más sólidos, esto sin la necesidad de tener un amplio conocimiento análisis de riesgo.

Esta metodología se enfoca principalmente en los activos de información, en cómo se almacenan, transportan, procesan y como están expuestos a las amenazas y las vulnerabilidades. A continuación se muestran los ocho pasos con los que cuenta esta metodología los mismos que están divididos en cuatro grupos

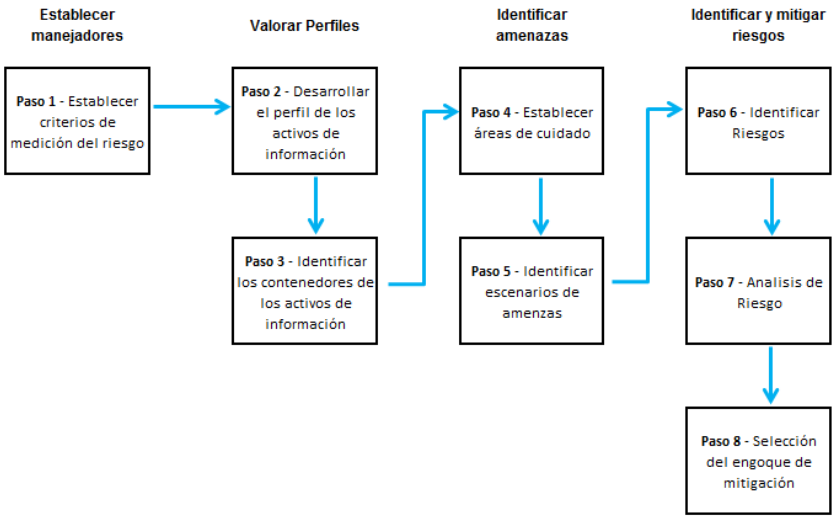


Figura 2.3 OCTAVE Allegro Mapa de Caminos

El primer paso se basa en determinar a los conductores de la organización los cuales serán usados para la evaluación de los efectos del riesgo en la misión y visión de la organización. Los conductores son ubicados en un conjunto de criterios de medición del riesgo, estos criterios son un conjunto de medidas cualitativas contra los cuales se medirá el efecto de un riesgo para finalmente formar la base de evaluación de riesgo de activos de información.

En el segundo paso, se debe realizar los perfiles de los activos de información, se debe considerar las características, cualidades y el valor del activo.

En el tercer paso, se describen los lugares donde los activos de información son almacenados, transportados y procesados también indicara si están o no bajo el control directo de la organización.

En el cuarto paso, se inicia el proceso con una lluvia de ideas sobre las posibles situaciones que puedan poner en riesgo un

activo de información, el propósito de este paso no es capturar una lista completa de todos los posibles escenarios de amenaza para un activo de información en cambio, la idea es capturar rápidamente aquellas situaciones o condiciones que vienen inmediatamente a la mente del equipo de análisis.

En el paso quinto, se considera con más detalle los escenarios tratados en el paso cuatro pero esta consideración no es tan robusta por lo cual en la etapa dos del paso cinco se consideran un rango más amplio de amenazas.

En el sexto paso, se realiza el análisis para determinar el impacto que puede causar una amenaza si estas se cumplen.

En el séptimo paso, se realiza un cálculo cualitativo para determinar como la organización es impactada por una amenaza.

En el octavo paso, se trata de priorizar el riesgo identificado de tal manera que se pueda mitigar se debe desarrollar una estrategia en la cual se considere el valor de activo, sus requerimientos de seguridad, sus contenedores, y su ambiente de operación [2].

2.3.2 METODOLOGIA MAGERIT

El Consejo Superior de la Administración Electrónica (CSAE) ha elaborado y promueve la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Magerit) como respuesta a la percepción de que la administración pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la Información.

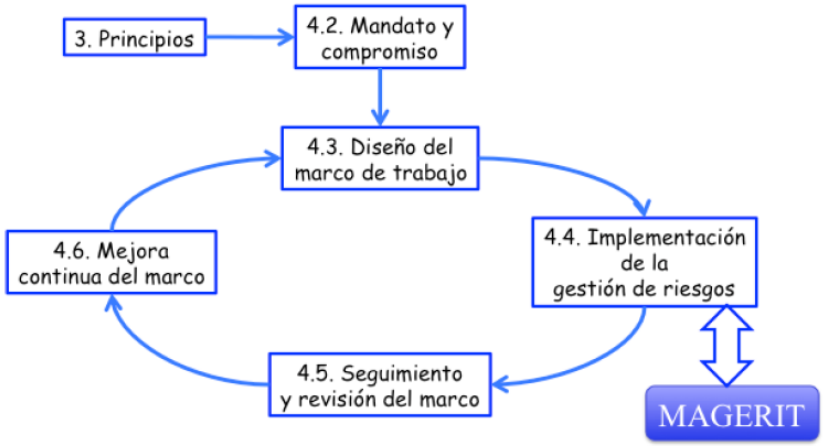


Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Figura 2.4 Marco de Trabajo para la gestión de riesgos de MAGERIT

La Metodología Magerit persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

> Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso (Tomado de: Magerit V3 libro 1, pág. 7)

Actividades de análisis y gestión de riesgos:

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.

Declaración de aplicabilidad

Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

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. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

Cumplimiento de normativa

Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

Plan de seguridad

Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos

Organización de las guías

Esta versión 3 de Magerit se ha estructurado en dos libros y una guía de técnicas:

— Libro I – Método

— Libro II – Catálogo de elementos

— Guía de Técnicas Recopilación de técnicas de diferente tipo que pueden ser de utilidad para la aplicación del método [4].

2.3.3 METODOLOGIA ISO 27005

El estándar está definido por 12 cláusulas, siendo las 6 primeras donde se define los alcances, definiciones, resumen de la norma. Las actividades del proceso están definidas de la cláusula 7 a la 12 y en las cuales se detalla el proceso de gestión de riesgo de la información. Además contiene anexos con información general de la evaluación de riesgos, amenazas y vulnerabilidades.

Cada clausula está definida por cuatro partes.

Entrada

Identifica cualquier información necesaria para realizar la actividad.

Acción Describe la actividad.

Guía de implementación Proporciona guía para realizar la acción. Algunas de estas guías no pueden será adecuadas para todos los casos y en otros serían las adecuadas.

Salida

Identificar cualquier información después de la actividad realizada.

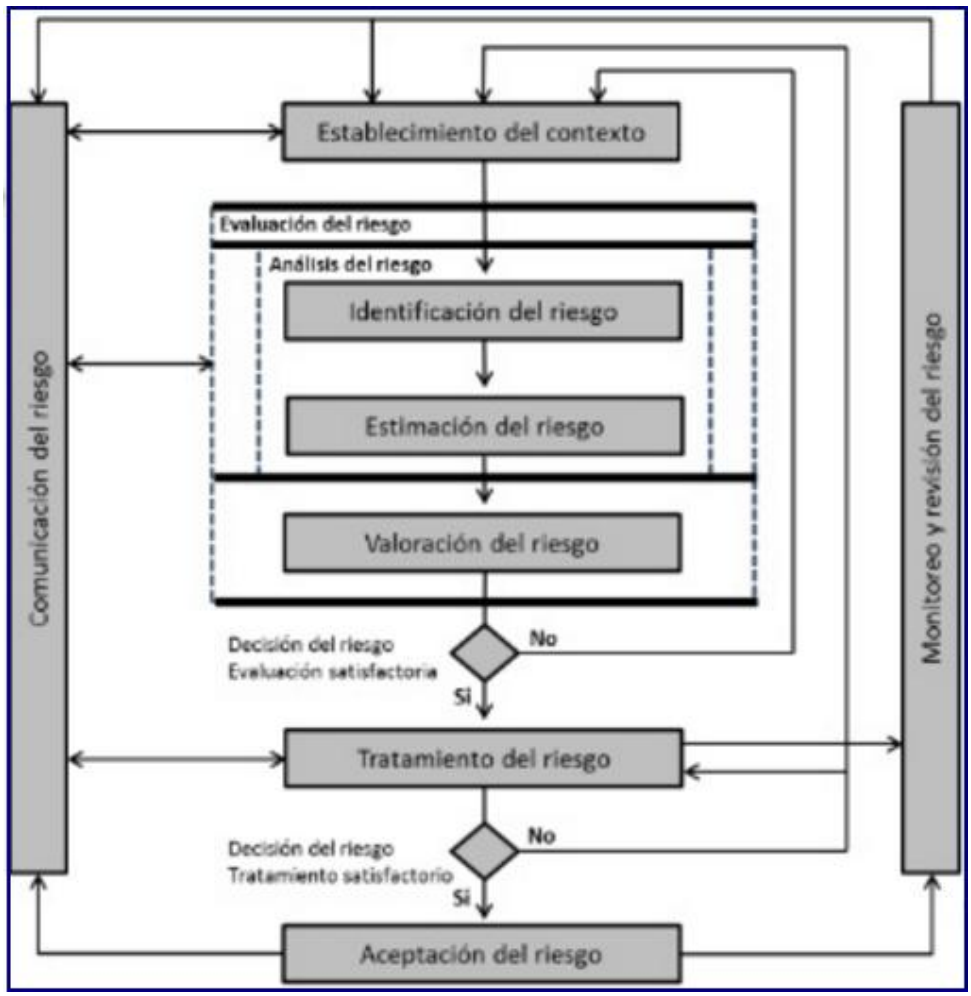


Figura 2.5 Ciclo de Trabajo de la ISO 27005

Criterios Básicos

Estos criterios dependerán del alcance y los objetivos que se planteen dentro de la organización, es por ello que es necesario en primera instancia desarrollar los criterios de aceptación del riesgo. Se debe considerar los recursos y la disponibilidad de los mismos ya que estos generan costos para la organización.

Los recursos asignados deberán realizar la valoración del riesgo y sus planes de tratamiento. También deben desarrollar e implementar las políticas en función de los controles seleccionados, monitorear si los controles está cumpliendo su función así como también deberán monitorear los procesos

CRITERIOS DE EVALUACION DEL RIESGO

Los criterios para la evaluación deben considerar lo siguiente:

- Que activos de información son más críticos.
- Los requisitos legales.

- La disponibilidad, confidencialidad e integridad de la información.
- El efecto en la reputación de la organización.

CRITERIOS DE IMPACTO

- Clasificación de los activos de información.
- Operaciones.
- Incumplimiento por fechas limite
- Incumplimiento de requisitos legales.

CRITERIOS DE LA ACEPTACION DEL RIESGO

Para la aceptación del riesgo se debe considerar el costo de una solución versus el costo de que el riesgo se materialice. Si el costo de que el riesgo se materialice es menor que el de la solución las organizaciones optan por aceptar el riesgo.

Se debe tener una clasificación de niveles en el cual todo riesgo que caiga en el nivel más bajo será el que se acepte [5].

2.4 ESTANDAR ISO/IEC 27002

ISO/IEC 27002:2013 código de buenas prácticas para la gestión de la Seguridad. Recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización Describe los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y especifica los controles recomendables a implantar (medidas a tomar).

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que

estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

ISO continúa desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

Toda la información disponible públicamente sobre el desarrollo de las normas de la serie 27000 puede consultarse en las páginas web del subcomité JTC1/SC27: 1 y 2).

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondo norma ISO/IEC 27002), Argentina (IRAM-ISO-IEC27002), Chile (NCh-

SO27002),Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799). El original en inglés y su traducción al francés pueden adquirirse en iso.org.

Actualmente, la última edición de 2013 del estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013 [6][11].

2.5 SELECCIÓN DEL MÉTODO DE ANÁLISIS DE RIESGO

Para la selección de la metodología se ha considerado las variables de costo y tiempo así como el factor experiencia que exige la metodología, también se tomará en cuenta el recurso humano que se necesita para llevar a cabo el análisis.

Metodologia	Costo (tiempo de analisis)	Costo (economico)	Equipo de trabajo	Experienia en analisis de riesgo	plantillas
Octave Allegro	alto	gratis	1 persona por area y jefes	no requerida	si
Magerit	alto	gratis	5 personas de cada area	no requerida	si
Iso27005	alto	gratis	1 persona por area y jefes	requerida	no

Figura 2.6 Comparación entre las metodologías revisadas

La variable equipo de trabajo representa un tiempo alto de análisis y reuniones pero ya que la aplicación será en el departamento de sistemas

las mismas se pueden concretar sin tener que realizar un gran esfuerzo en coordinación con las áreas y personas involucradas.

Otro factor importante es la facilidad en el uso de la metodología, una de ellas es que cuenta con un conjunto de plantillas y una serie de pasos detallados para su aplicación, lo cual agilita el proceso durante las reuniones, y por último se tomara en cuenta la experiencia que se requiere para la implementación.

Por lo antes mencionado la metodología seleccionada es Octave Allegro y luego de ello se procederá con el análisis correspondiente siguiendo los pasos que indica la metodología.

CAPÍTULO 3

SITUACION ACTUAL

3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD INFORMÁTICA DEL DS.

En la situación actual del DS (Departamento de Sistemas) se va a detallar la organización del departamento por áreas, así como se indicaran los activos de información que posee el departamento y por último se realizará una encuesta al personal del DS que tenga más de 1 año de antigüedad con el fin de poder determinar la situación actual del departamento en lo referente a conocimientos de seguridad informática.

En la actualidad el DS carece de un manual que determine las normas y procedimientos relacionados a la seguridad de la información, lo que

genera entre otras la falta de eficiencia y efectividad de las actividades que se desarrollan

El DS se encuentra conformado por 4 áreas que son Soporte, Desarrollo de Software, Infraestructura, Control de Calidad. Cada una de estas áreas cuenta con su jefatura las cuales reportan a la gerencia.

Dentro del área de desarrollo se encuentran el proceso de desarrollo propio y el desarrollo por parte de personal externo, en el caso de los desarrollos propios estos luego de ser terminados pasan al área de control de calidad.

El área de soporte cuenta con 2 niveles que son mesa de ayuda, soporte de hardware y soporte de aplicaciones

En el área de infraestructura se encuentra el personal de operaciones, de comunicaciones y de manejo de base de datos.

3.2 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

El proceso de identificación de activos de información es muy importante, ya que nos permite reconocer cuales son los activos que se encuentran asociados a los procesos de la organización. La realización de cada proceso involucra activos de información específicos, a continuación se lista los activos:

Tabla 3 Descripción de los activos

	Tipo de Activo	Descripción
1	Sistemas de información	Sistema de ventas, sistema Interno de administración y Sistema bodega
2	Documentos	Requerimientos, Pases de Versión, Memorias Técnicas
3	Recursos Humanos	Personal, Proveedores
4	Hardware	PC, Laptops, Servidores, Impresoras, Teléfonos IP
5	Software	Ofimática, Base de Datos, Herramientas de desarrollo
6	Terceros	Internet , copiadoras

3.3 ESTADÍSTICA ACTUAL

En esta sección evaluaremos mediante una encuesta al personal del DS con el fin de obtener retroalimentación sobre cómo se maneja la seguridad de la información en sus diferentes áreas.

En un total son 40 personas que están divididas de la siguiente forma.

- 5 Operaciones
- 2 Administradores de Bases
- Comunicación
- 6 Soporte II
- 8 Soporte I
- Soporte H/S
- 10 desarrollo
- 5 Control de Calidad

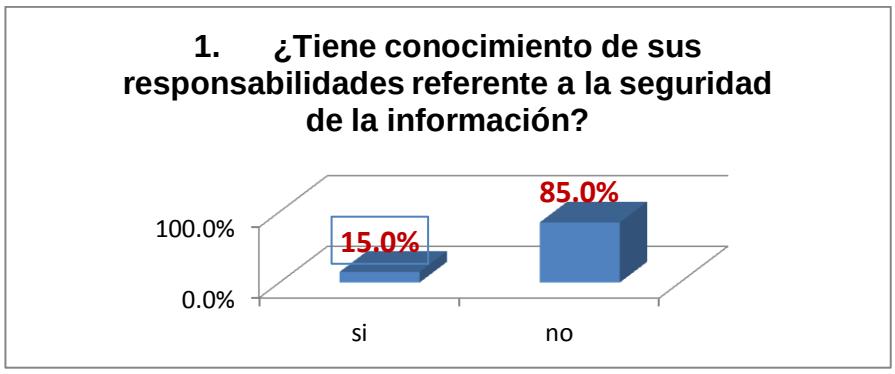


Figura 3.1 Encuesta Pregunta 1

El personal del DS indico en un 85% que no tienen de sus responsabilidades frente a la seguridad de la información. También indicaron que no se les ha proporcionado un manual con los lineamientos de seguridad informática de la empresa.

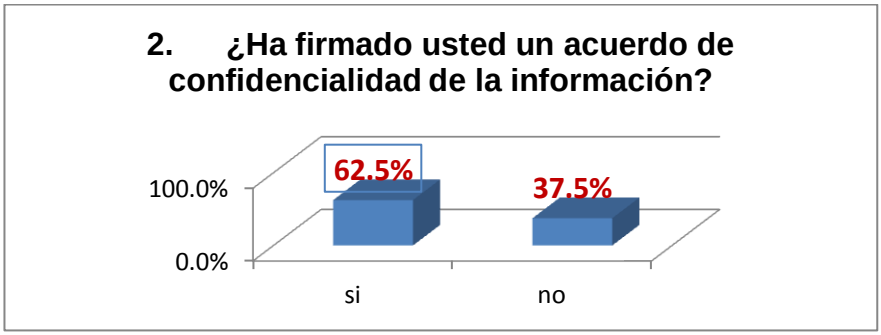


Figura 3.2 Encuesta Pregunta 2

El 62.5% del personal del departamento indico que si han firmado un acuerdo de confidencialidad, pero el mismo solo aplica sobre los códigos de programación utilizados o vistos en los desarrollos. El porcentaje restante a pesar de tener ya más de 1 año en el departamento mantiene firmado el acuerdo de confidencialidad.

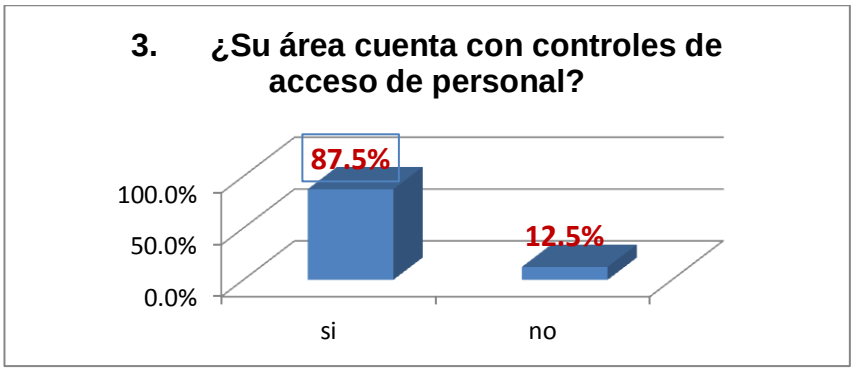


Figura 3.3 Encuesta Pregunta 3

Existe un acceso interno por el cual cualquier persona de la empresa puede entrar al DS. El control esta puesto para terceras personas ya que deberán pasar por un acceso biométrico si requieren ingresar.

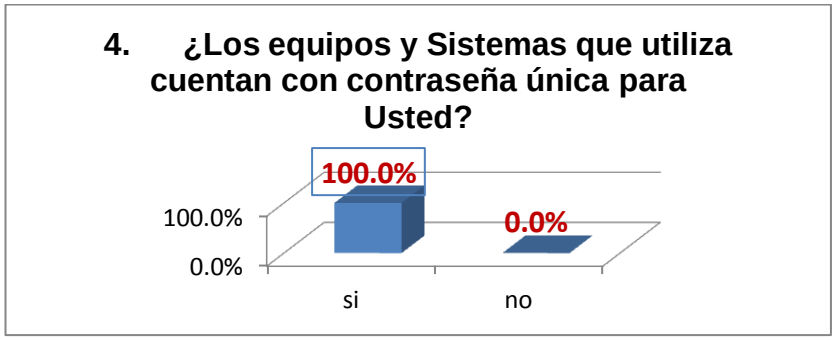


Figura 3.4 Encuesta Pregunta 4

Todo el personal del DS cuenta con su propio acceso a su respectivo equipo esto es manejado por un directorio activo y controlado por el área de infraestructura.

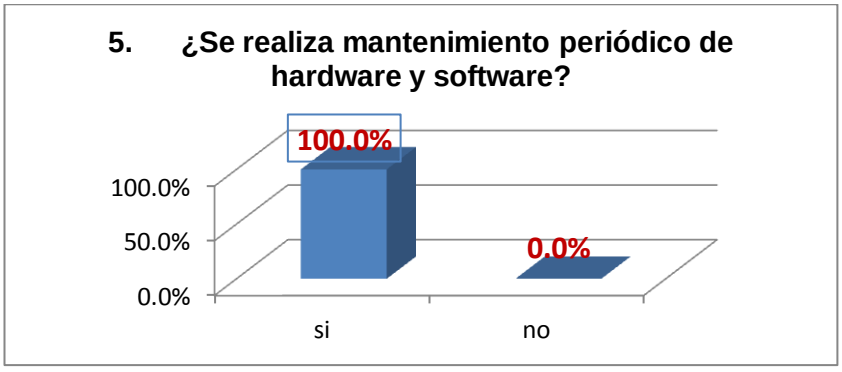


Figura 3.5 Encuesta Pregunta 5

Si bien los equipos del DS cuentan con un antivirus estos nos son actualizados regularmente, tampoco se realizan actualizaciones de los sistemas operativos. Lo cual deja brechas de seguridad que ya fueron parchadas por el propio Microsoft y que no se están aplicando.

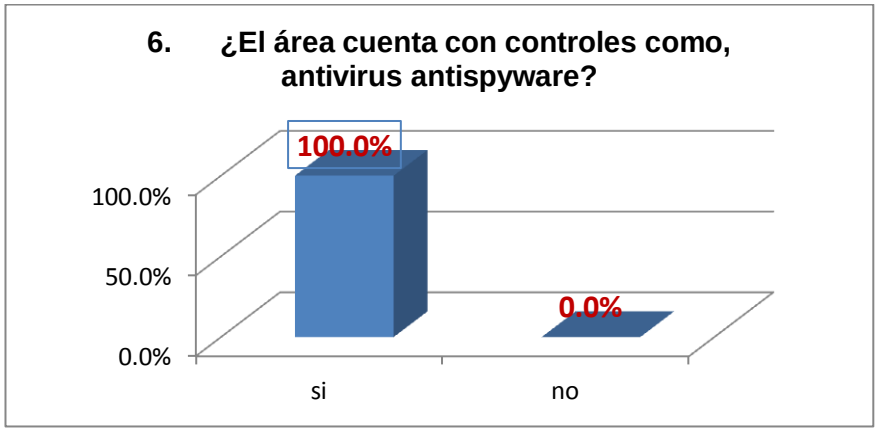


Figura 3.6 Encuesta Pregunta 6

Todos los equipos cuentan con sistema de antivirus y antispyware.

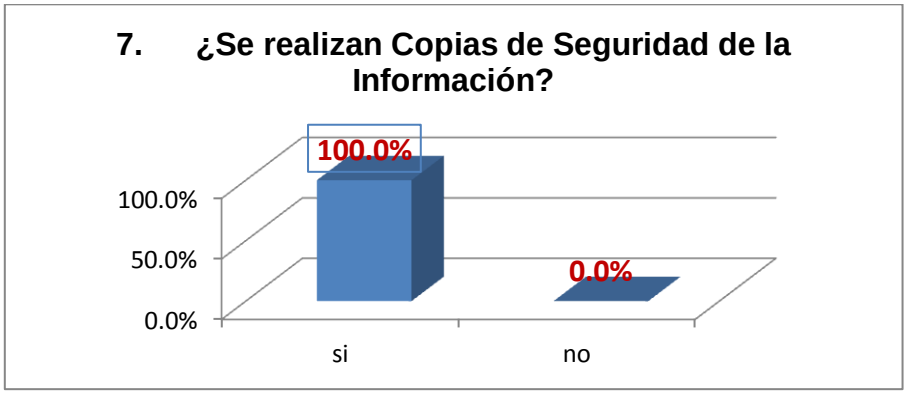


Figura 3.7 Encuesta Pregunta 7

El departamento de operaciones indica que los respaldos de la información se realizan de forma semanal y se indica que los respaldos se realizan en cintas (preguntas 8, 9).

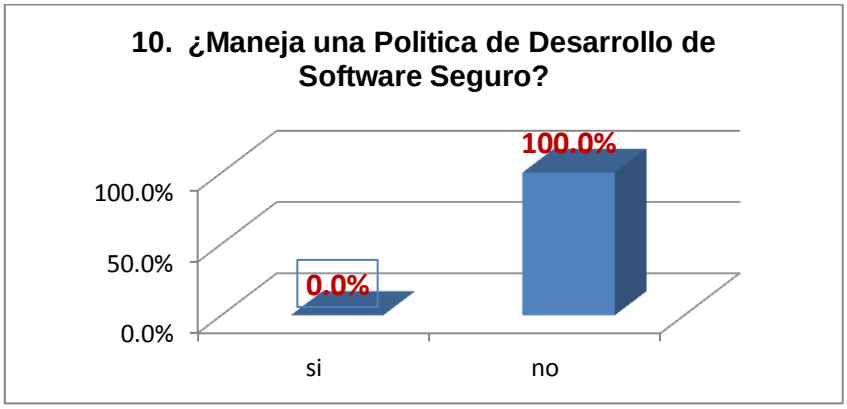


Figura 3.8 Encuesta Pregunta 8

Las personas del departamento indicaron en un 100% del personal indica no conocer de la existencia de este tipo de políticas.

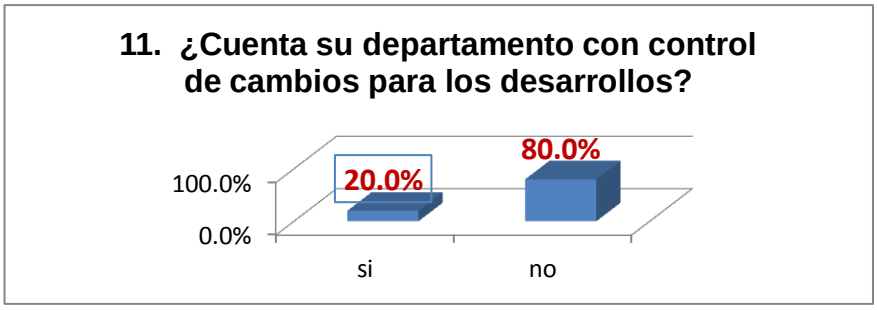


Figura 3.9 Encuesta Pregunta 9

Los controles de cambios son utilizados por el personal de desarrollo y de control de calidad para mantener un historial de todas las modificaciones que se realizan a los desarrollos internos. El 80% de los desarrolladores indican que existe un manual de control de cambios pero el mismo no lo utilizan debido a la falta de tiempo con la que terminan sus proyectos. Mientras que el personal de control de calidad indica que ellos aplican el manual para los desarrollos que provienen del sistema de ventas.

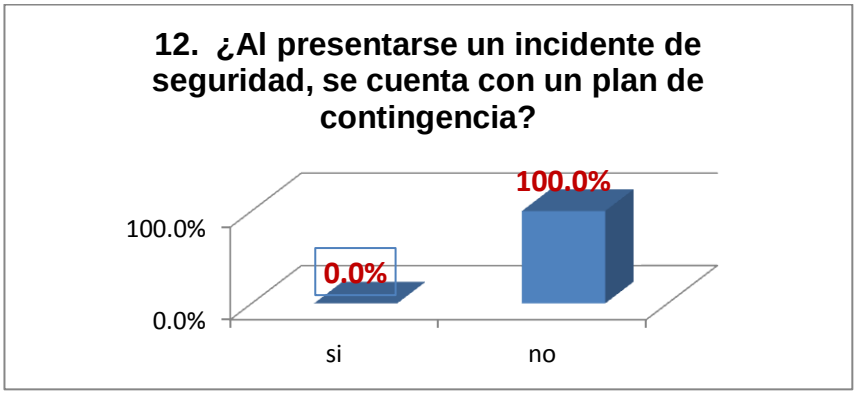


Figura 3.10 Encuesta Pregunta 10

El personal del DS no tiene conocimiento de lo que es un plan de contingencia y en que situaciones se debe aplicar.

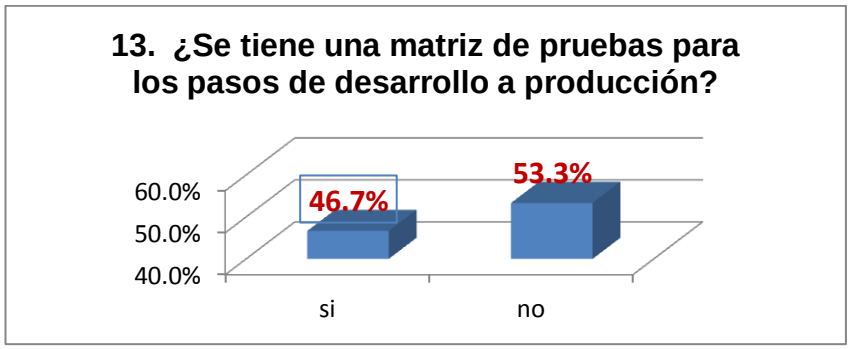


Figura 3.11 Encuesta Pregunta 11

Aunque el personal indica que cuentan con una matriz de pruebas el 53.3% indica que esta matriz no es insuficiente ya que no abarca todos los puntos a evaluar sobre los requerimientos planteados.

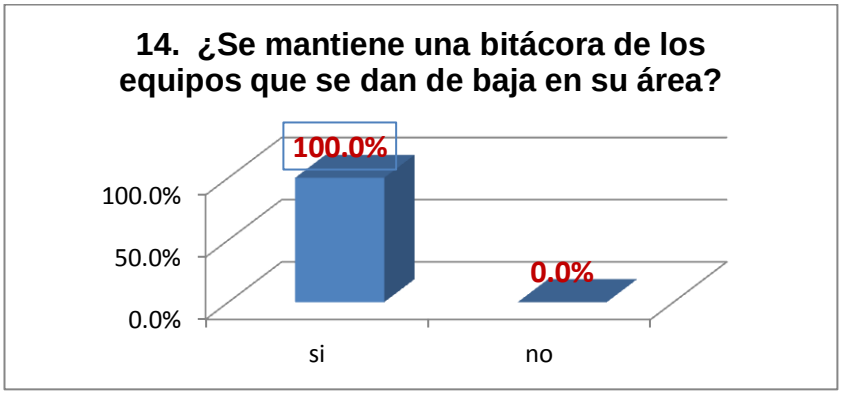


Figura 3.12 Encuesta Pregunta 12

El área que maneja los equipos (soporte de hardware) mantiene una bitácora de todo el equipo que se dan de baja y de todos los que se asignan al personal del departamento.

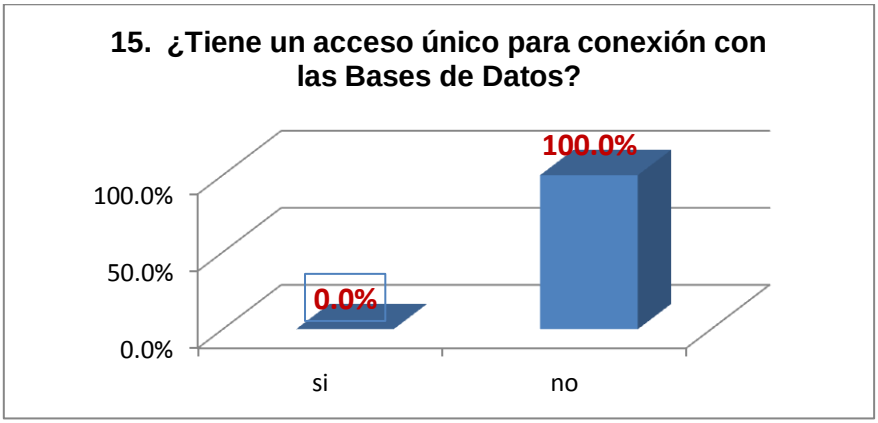


Figura 3.13 Encuesta Pregunta 13

El 100% de los usuarios indicaron que a los servidores de base de datos se ingresa con el usuario por defecto y que existe otro usuario el mismo que es utilizado por todos los del departamento tanto en desarrollo como en producción.

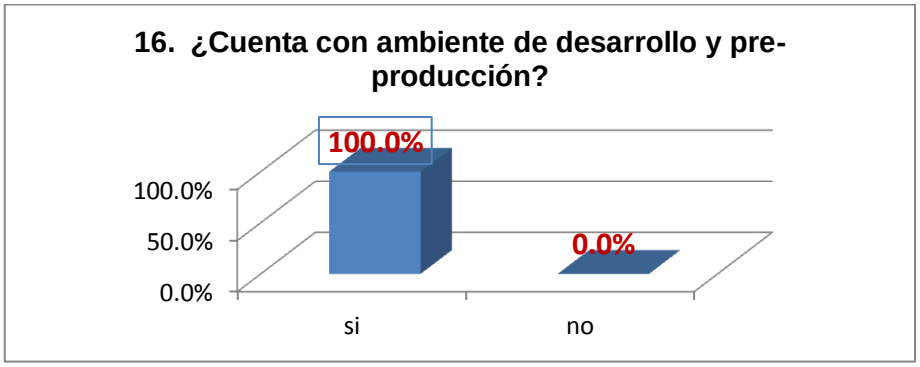


Figura 3.14 Encuesta Pregunta 14

El departamento cuenta con 3 tipos de ambientes, desarrollo, pruebas y producción, y el 100% de los usuarios están al tanto de esto para sus desarrollos pruebas y monitoreo.

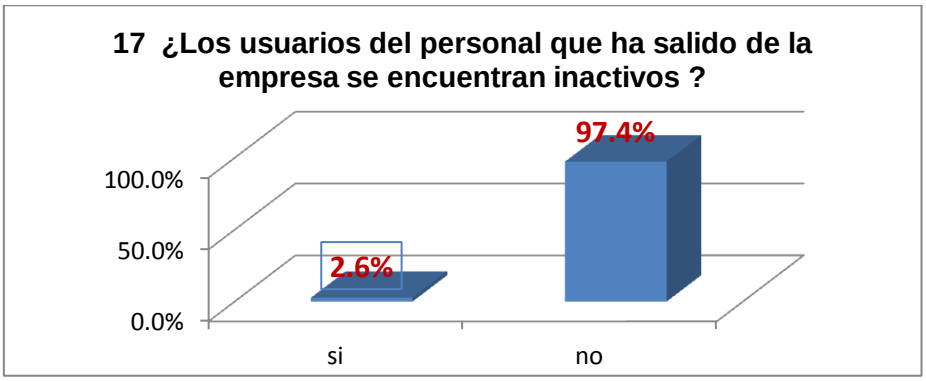


Figura 3.15 Encuesta Pregunta 15

El 97.4% de los encuestados indicaron que para su trabajo utilizan usuarios de personas que ya no trabajan en la empresa.

3.4 INVENTARIO DE ACTIVOS

El DS cuenta con activos que serán listados en la siguiente tabla, entre los cuales se encuentran PC , teléfonos IP, antivirus , programas de ofimática y la ubicación de los mismos

Tabla 4 Activos de la organización

Ubicación	Tipo	Marca	Antivirus	Ofimática	Cantidad
Desarrollo	Escritorio	HP	Kaspersky	Office 2010	10
Infraestructura	Laptop	HP	Kaspersky	Office 2010	3
Calidad	Impresora	Canon			1
Calidad	PC	HP	Kaspersky	Office 2010	5
Soporte I	PC	HP	Kaspersky	Office 2010	8
Soporte H/S	Laptop	HP	Kaspersky	Office 2010	3
Desarrollo	Teléfono	Cisco			1
Infraestructura	Teléfono	Cisco			3
Calidad	Teléfono	Cisco			1
Soporte I	Teléfono	Cisco			1
Sistema V.	Servidor	HP	Kaspersky	Office 2010	1
Sistema L	Servidor	HP	Kaspersky	Office 2010	1

CAPÍTULO 4

ANÁLISIS

4.1 ANÁLISIS DE LA NORMA APLICADA AL DEPARTAMENTO

La norma que se aplicara en el DS es la ISO/IEC 27002 la cual es un estándar de seguridad de la información, la cual proporciona las mejores prácticas a considerar para cuando se desea implementar o mantener un sistema de gestión de la seguridad de la información.

Esta norma al ser un estándar internacional es aplicable a cualquier institución, es de fácil entendimiento, manejo y adaptación en una organización. No es una norma certificable ya que no especifica los requisitos necesarios para una certificación.

La ISO/IEC 27002 entrega de forma detalladas la información de cada uno de sus controles lo que ayuda de sobremanera a su entendimiento y aplicación, adicional esta norma es ideal si lo que se desea es colocar controles de seguridad.

En conclusión a pesar de no ser una norma certificable la ISO/IEC 27002 ofrece lo que el DS necesita para la implementación de controles para el fácil entendimiento por parte de los usuarios.

4.2 SELECCIÓN DE CONTROLES BASADOS EN EL ESTÁNDAR ISO/IEC 27002

Con los datos obtenidos en la encuesta se procede a determinar el dominio y el control de la norma con el cual vamos a trabajar los diferentes puntos [7][8].

Tabla 5 Relación entre la encuetas y los controles de la norma

Pregunta	Dominio	Control
¿Tiene conocimiento de sus responsabilidades referente a la seguridad de la información?	Control de Acceso	9.3
¿Ha firmado usted un acuerdo de confidencialidad de la información?	Control de Acceso	9.3
¿Los equipos y Sistemas que utiliza cuentan con contraseña única para Usted?	Control de Acceso	9.4
¿Se realizan Copias de Seguridad de la Información?	Gestión de activos	8.3
¿En qué medio se almacenan los respaldos? Cintas	Gestión de activos	8.3
¿Con que periodicidad se realizan? Semanalmente	Gestión de activos	8.3
¿Maneja una Política de Desarrollo de Software Seguro?	Ad. Des. Mant. Software	14.2
¿Cuenta su departamento con control de cambios para los desarrollos?	Ad. Des. Mant. Software	14.2
¿Se tiene una matriz de pruebas para los pasos de desarrollo a producción?	Ad. Des. Mant. Software	14.2
¿Se mantiene una bitácora de los equipos que se dan de baja en su área?	Gestión de activos	8.1
¿Tiene un acceso único para conexión con las Bases de Datos?	Control de Acceso	9.4
¿Cuenta con ambiente de desarrollo y pre-producción?	Ad. Des. Mant. Software	14.2
¿Los usuarios del personal que ha salido de la empresa se encuentran inactivos?	Control de Acceso	9.2

4.2.1 CONTROLES DE MANEJO DE ACTIVO

El manejo de activos tiene como principal objetivo que la organización tenga conocimiento preciso sobre los activos de información y sobre su clasificación a nivel de criticidad y sensibilidad según la información que manejan.

Se conoce como activos a las base de datos, documentación, manuales, procedimiento, aplicaciones, sistemas operativos, herramientas de desarrollo, hardware.

Se debe considerar que la clasificación de un ítem de información determinado puede variar en el tiempo, según las prioridades de la organización por lo que es importante tener un esquema de clasificación sencillo, adaptable y aplicable.

Los controles que la norma indica son:

1. Responsabilidad sobre los activos.
2. Clasificación de la información.
3. Manejo de los soportes de almacenamiento.

4.2.2 CONTROLES DE CONTROL DE ACCESOS

El objetivo del presente dominio es controlar el acceso a través de restricción o procedimientos, que limiten el acceso a información o que controlen la asignación critica., con el fin de impedir el acceso no autorizado a los sistemas de información. Estos procedimientos deben ser documentados, comunicados y difundidos.

Los procedimientos deben contemplar los accesos de los usuarios, desde el registro hasta la terminación de las actividades para las cuales requieren el acceso.

Los controles que la norma indica son:

- Requisitos de negocio para el control de accesos.
- Gestión de acceso de usuario.
- Responsabilidades del usuario.
- Control de acceso a sistemas y aplicaciones.

4.2.3 CONTROLES DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Los controles que la norma indica son:

- Requisitos de seguridad de los sistemas de información.
- Seguridad en los procesos de desarrollo y soporte.
- Datos de prueba.

4.2.4 RELACIÓN ENTRE LA REDUCCIÓN DEL RIESGO Y LA IMPLEMENTACIÓN DE CONTROLES

La organización debe tomar la decisión de que controles implementar en función de sus necesidades o prioridades, o puede implementar sus propios controles dependiendo de la experiencia que se ha obtenido a lo largo del tiempo[10]

La implementación de controles se relaciona con el riesgo estimado en dos maneras:

1. Reduciendo la posibilidad de que la vulnerabilidad sea explotada.

2. Reduciendo el impacto si el riesgo se materializa

La organización debe seleccionar con cuál de estos esquemas trabajar o usar una combinación de ambas, esto dependerá del control así como de la estrategia de aceptación del riesgo. Esta decisión depende en ocasiones del giro del negocio.

En conclusión los métodos que se seleccionen involucran decisiones y consultas, entre las áreas de una organización y en otros casos depende de los dueños de los activos y de la criticidad con la que deseen asegurar su información.

4.3 ESTABLECIMIENTO DEL CRITERIO DE MEDICION DEL RIESGO

El criterio de medición de riesgo seleccionado es Octave Allegro, este método considera la misión de la organización y los objetivos ya que estos son los que se verán afectados si una amenaza se materializa.

Misión: Brindar servicios y productos farmacéuticos que contribuyan con el bienestar de la comunidad, de manera integrada, responsable.

Los niveles definidos como baja, media y alta son propias del estándar. Los valores Cualitativos de los niveles son con los que se podrá evaluar el efecto de un riesgo en la misión y objetivos estratégicos.

Para la reputación se tomaron los valores predefinidos en el método por lo tanto estos valores son tomados desde el menor porcentaje posible 10% y manteniendo la proporción de porcentaje.

Tabla 6 Área de impacto Reputación y confianza

	REPUTACION Y CONFIANZA		
Área de Impacto	**Baja**	**Media**	**Alta**
Reputación	Tiene una afectación mínima	Se requiere poco esfuerzo para recuperarse del daño	La reputación se afecta completamente
Credibilidad	menos del 10% de reducción	Entre 10%y 20% de reducción de la credibilidad	Más del 20% de reducción de la credibilidad
Social	N/A	N/A	N/A

Tabla 7 Área de impacto Productividad

	REPUTACION Y CONFIANZA		
Área de Impacto	**Baja**	**Media**	**Alta**
Horas de Personal	1 hora o menos	De 1 a 2 horas sin algún servicio	De 3 horas en adelante sin algún servicio

Esta área de impacto está enfocada principalmente a personal que dependen de los servicios que se están analizando, de la experiencia de las operaciones diaria, se ha tomado como unidad 1 hora para definir molestia y se ha incrementado de manera proporcional hasta llegar a la tercera hora. Cabe indicar que estos valores son relativos porque

depende del tipo de personal y del departamento de la empresa afectado.

Se ha tomado como prioridad más alta al área de impacto de reputación y de confianza ya que es aquí donde se debe cumplir con la misión y objetivos estratégicos, es decir, mantener una gestión ágil en lo que es relacionado a las ventas puesto que con la alta competencia que existe el cliente es muy susceptible a cambiar de proveedor o de servicio.

Tabla 8 Priorización de las Áreas de Impacto

	Priorización de las Áreas de Impacto
Prioridad	**Áreas de Impacto**
2	Reputación y confianza
1	Productividad
N/A	Cumplimiento de regulaciones
N/A	Seguridad y Salud

El siguiente paso es justificar la selección del activo de información, en esta fase se determinan los activos de información más importantes para la Organización.

- La información que genera el sistema de ventas

- La información que se genera desde el sistema interno
- La información que recibe el sistema de bodega
- La información que maneja el sistema de Soporte de incidentes

También se define los propietarios del activo de información así como los requerimientos de seguridad de la información e indicando cuál de ellos es el más importante para ese activo.

4.4 DESARROLLO DE PERFILES DE ACTIVOS DE INFORMACIÓN

Octave –Allegro nos presenta una plantilla en la cual se debe justificar el activo de información que se está seleccionando como crítico. En las plantillas se colocara los activos críticos.

A continuación se detalla la plantilla de los activos conocidos como sistema de ventas, sistema comercial y sistema de bodega, que son los sistemas críticos.

Estos sistemas fueron seleccionados debido a la importancia que tienen dentro de las operaciones diarias ya que son el núcleo del negocio.

En esta fase se determinan los activos de información más importante y también se define a los propietarios de los activos y sus requerimientos de seguridad.

Tabla 9 Octave-Allegro Hoja de Trabajo #8

Perfil de activos información crítica			
Activo Critico	**Justificación Selección ¿Por qué este activ0 de información es importante para la organización?**		**Descripción**
Información del sistema de Ventas	Porque es el principal medio utilizado para las actividades relacionados con la venta directa a los clientes y su información		Sistema de ventas
Propietarios			
Persona:	Jefe de Sistemas		
Área:	Área de Desarrollo		
Requerimientos de Seguridad			
Confidencialidad	X	Solo personal autorizado debe acceder a este activo	Solo usuarios que cuenten con su respectivo usuario y clave pueden tener acceso al activo
Disponibilidad	X	Este activo debe estar disponible para los usuarios. Este activo debe estar disponible 24/7 durante 365 días al año	Solo los usuarios con acceso al sistema pueden hacer uso del mismo en los periodos de tiempo establecidos
Integridad	X	Solo personal autorizado puede modificar este activo	
¿Cuál es el requisito de seguridad más importante para este activo de información?			
Confidencialidad √	Disponibilidad √	Integridad √	Otro

Tabla 10 Octave-Allegro Hoja de Trabajo #8

Perfil de activos información crítica			
Activo Critico	**Justificación Selección ¿Por qué este activo de información es importante para la organización?**		**Descripción**
Información del sistema comercial	Porque es el principal medio utilizado para las actividades relacionadas con el registro de la información de los clientes y las negociaciones con la organización		Sistema Interno
Propietarios			
Persona:	Jefe de Sistemas		
Área:	Área de Desarrollo		
Requerimientos de Seguridad			
Confidencialidad	X	Solo personal autorizado debe acceder a este activo	
Disponibilidad	X	Este activo debe estar disponible para los usuarios. Este activo debe estar disponible 8h de lunes a viernes	Solo los usuarios con acceso al sistema pueden hacer uso del mismo en los periodos de tiempo establecidos
Integridad	X	Solo personal autorizado puede modificar este activo	
¿Cuál es el requisito de seguridad más importante para este activo de información?			
Confidencialidad √	Disponibilidad √	Integridad √	Otro

Tabla 11 Octave-Allegro Hoja de Trabajo #8

Perfil de activos información crítica			
Activo Critico	**Justificación Selección ¿Por qué este activo de información es importante para la organización?**		**Descripción**
Información del sistema de Bodega	Porque es el principal medio utilizado para las actividades relacionados con logística de los productos que maneja la organización		Sistema de Bodega
Propietarios			
Persona:	Jefe de Sistemas		
Área:	Área de Desarrollo		
Requerimientos de Seguridad			
Confidencialidad	X	Solo personal autorizado debe acceder a este activo	Solo usuarios que cuenten con su respectivo usuario y clave pueden tener acceso al activo
Disponibilidad	X	Este activo debe estar disponible para los usuarios. Este activo debe estar disponible 24/7 durante 365 días al año	Solo los usuarios con acceso al sistema pueden hacer uso del mismo en los periodos de tiempo establecidos
Integridad	X	Solo personal autorizado puede modificar este activo	

¿Cuál es el requisito de seguridad más importante para este activo de información?			
Confidencialidad √	Disponibilidad √	Integridad √	Otro

4.5 IDENTIFICAR LOS CONTENEDORES DE LOS ACTIVOS DE INFORMACIÓN

Ahora se procederá a identificar los contenedores de los activos de información. Un contenedor es, donde un activo de información es almacenado, transportado, o procesado. En este caso se evaluaran los activos tecnológicos y las personas como contenedores del activo. Se utilizan las plantillas Octave-Allegro 9a (activos tecnológicos), y 9c (personas). Para cada servicio se identifica sus contenedores internos y externos de manera detallada.

- Contenedores técnicos del activo de información: Sistema de Ventas
- Personas como Contenedores técnicos de información
- Contenedores técnicos del activo de información: Sistema Interno
- Personas como Contenedores técnicos de información
- Contenedores técnicos del activo de información: Sistema de Bodega
- Personas como Contenedores técnicos de información

Tabla 12 Octave-Allegro Hoja de Trabajo #9A

9A	Contenedores técnicos del activo de información: Sistema de Ventas	
Internos		
Descripción		**Propietario**
La información es procesada en el servidor designado como contenedor del sistema de ventas		TI
Desde la PC del Cliente la información es transportada por la LAN de la organización y se guarda en el servidor asignado al sistema de ventas		TI
La información de autenticación es configurada en cada PC con un usuario y una contraseña		TI
Externos		**Propietario**
La información es transportada a los usuarios externos a través del internet		CNT
Personal de soporte del proveedor, en cual está estimado a resolución de problemas en los diferentes servidores donde se encuentra el activo de información		IBM

Tabla 4.8 Octave-Allegro Hoja de Trabajo #9C

9C	Personas como Contenedores técnicos de información	
Internos		
Descripción		**Propietario**
DBA		TI
Personal de infraestructura		TI
Personal de Soporte Técnico		TI
Externos		**Propietario**
N/A		N/A

Tabla 13 Octave-Allegro Hoja de Trabajo #9A

9A	Contenedores técnicos del activo de información: Sistema Interno
Internos	
Descripción	**Propietario**
La información es procesada en el servidor designado como contenedor del sistema interno	TI
Desde la PC del Cliente la información es transportada por la LAN de la organización y se guarda en el servidor asignado al sistema de ventas	TI
La información de autenticación es configurada en cada PC con un usuario y una contraseña	TI
Externos	**Propietario**
Personal de soporte del proveedor, en cual está estimado a resolución de problemas en los diferentes servidores donde se encuentra el activo de información	IBM

Tabla 14 Octave-Allegro Hoja de Trabajo #9C

9C	Personas como Contenedores técnicos de información
Internos	
Descripción	**Propietario**
DBA	TI
Personal de infraestructura	TI
Personal de Soporte Técnico	TI
Externos	**Propietario**
N/A	N/A

Tabla 15 Octave-Allegro Hoja de Trabajo #9A

9A	Contenedores técnicos del activo de información: Sistema de Bodega
Internos	
Descripción	**Propietario**
La información es procesada en el servidor designado como contenedor del sistema de bodega	TI
Desde la PC del Cliente la información es transportada por la LAN de la organización y se guarda en el servidor asignado al sistema de bodega	TI
La información de autenticación es configurada en cada PC con un usuario y una contraseña	TI
Externos	**Propietario**
La información es transportada a los usuarios externos a través del internet	CNT
Personal de soporte del proveedor, en cual está estimado a resolución de problemas en los diferentes servidores donde se encuentra el activo de información	IBM

Tabla 16 Octave-Allegro Hoja de Trabajo #9C

9C	Personas como Contenedores técnicos de información
Internos	
Descripción	**Propietario**
DBA	TI
Personal de infraestructura	TI
Personal de Soporte Técnico	TI
Externos	**Propietario**
N/A	N/A

4.6 IDENTIFICAR LOS ESCENARIOS DE AMENAZAS

El siguiente paso es identificar los escenarios de las posibles amenazas para ello se hace uso de los cuestionarios que nos proporciona la metodología lo cuales tratan de crear posibles escenarios que podrían afectar el activo de información en alguno de los contenedores descritos anteriormente. Los cuestionarios contemplan si el escenario positivo ocurre sea de manera accidental o intencional, y por último en el escenario 3 se revisan las preguntas que van dirigidas a indicar el tipo de impacto negativo que tendría la amenaza.

A continuación se presentan los cuestionarios los mismos que tendrán un fondo de color amarillo para marcar las respuestas

Tabla 17 Octave-Allegro Cuestionario #1

Cuestionario1 – Sistema de Ventas		**Contenedores Técnicos**	
Escenario1: Pensar acerca de las personas que trabajan en la Institución. ¿Hay una situación en la que un empleado podría acceder a uno o más contenedores técnicos, accidentalmente o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?	**No**	si (Accidentalmente)	si (intencionalmente)
Modificado así que no sea utilizable para los fines previstos?	No	**si (Accidentalmente)**	si (intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?	No	**si (Accidentalmente)**	Si (intencionalmente)
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?	**No**	si (Accidentalmente)	si (intencionalmente)
Escenario2: Pensar en personas que son externas a la Institución. Podría incluir a personas que tienen relación de negocio con la Institución o no. ¿ Hay alguna situación en la cual un externo podría acceder uno o más contenedores técnicos, accidental o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?	No	**Si (Accidentalmente)**	**Si (intencionalmente)**
Modificado así que no sea utilizable para los fines previstos?	**No**	si (Accidentalmente)	si (intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?	No	si (Accidentalmente)	**SI (intencionalmente)**
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?	**No**	si (Accidentalmente)	si (intencionalmente)

Tabla 18 Octave-Allegro Cuestionario #2

Cuestionario2		**Contenedores Técnicos**	
Escenario1: Pensar en las personas que trabajan en la Institución. ¿Hay una situación en la cual un empleado tiene conocimiento detallado de su activo de información y podría, accidental o intencionalmente, causar que el activo de información sea:			
Divulgado a personas no autorizadas?	No	**Si (Accidentalmente)**	**Si (intencionalmente)**
Modificado, de tal manera que no sea utilizable para los fines previstos.	**No**	si (Accidentalmente)	si (intencionalmente)
Interrumpido, así que no puede ser accedido para los fines previstos.	No	**si (Accidentalmente)**	Si (intencionalmente)
Permanentemente destruido o temporalmente perdido, así que no puede ser usado para los fines previstos.	No	**si (Accidentalmente)**	Si (intencionalmente)
Escenario2: Pensar en personas que son externas a la Institución. Esto podría personas quienes tienen una relación de negocio con la Institución o no. ¿Hay alguna situación en la cual un externo, accidental o intencionalmente, podría causar que el activo de información sea:			
Divulgado a personas no autorizadas?	No	**Si (Accidentalmente)**	**Si (intencionalmente)**

Tabla 19 Octave-Allegro Cuestionario #1

Escenario3: Considerar situaciones que podrían afectar el activo de información en cualquier contenedor técnico identificado. Determinar si cualquiera de las siguientes situaciones podría ocurrir, y si es afirmativo, determinar si estas situaciones podrían causar uno o más de los siguientes resultados. · La divulgación no intencional del activo de información. · La modificación no intencional del activo de información. · La interrupción no intencional de la disponibilidad del activo de información. · La destrucción permanente o temporal no intencional del activo de información.					
Un defecto de software.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Un fallo del sistema de origen conocido o desconocido.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Un defecto de hardware.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Código malicioso (virus, gusanos, Caballo de Troya, o puerta trasera) es ejecutado.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Fuente de energía de los contenedores es interrumpida	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Problemas con las telecomunicaciones.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Otros problemas de terceros o Sistemas.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Desastres naturales o causados por el hombre.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)

Tabla 20 Octave-Allegro Cuestionario #1

Cuestionario1 -SISTEMA INTERNO			**Contenedores Técnicos**
Escenario1: Pensar acerca de las personas que trabajan en la Institución. ¿Hay una situación en la que un empleado podría acceder a uno o más contenedores técnicos, accidentalmente o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?	**No**	si (Accidentalmente)	Si (intencionalmente)
Modificado así que no sea utilizable para los fines previstos?	No	**si (Accidentalmente)**	si (intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?	**No**	si (Accidentalmente)	Si (intencionalmente)
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?	**No**	si (Accidentalmente)	si (intencionalmente)
Escenario2: Pensar en personas que son externas a la Institución. Podría incluir a personas que tienen relación de negocio con la Institución o no. ¿ Hay alguna situación en la cual un externo podría acceder uno o más contenedores técnicos, accidental o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?	No	**Si (Accidentalmente)**	si (intencionalmente)
Modificado así que no sea utilizable para los fines previstos?	**No**	si (Accidentalmente)	si (intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?	**No**	si (Accidentalmente)	si (intencionalmente)
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?	No	**Si (Accidentalmente)**	si (intencionalmente)

Tabla 21 Octave-Allegro Cuestionario #2

Cuestionario2		**Contenedores Técnicos**	
Escenario1: Pensar en las personas que trabajan en la Institución. ¿Hay una situación en la cual un empleado tiene conocimiento detallado de su activo de información y podría, accidental o intencionalmente, causar que el activo de información sea:			
Divulgado a personas no autorizadas?	No	**si (Accidentalmente)**	**si (intencionalmente)**
Modificado, de tal manera que no sea utilizable para los fines previstos.	No	**si (Accidentalmente)**	**si (intencionalmente)**
Interrumpido, así que no puede ser accedido para los fines previstos.	No	**si (Accidentalmente)**	si (intencionalmente)
Permanentemente destruido o temporalmente perdido, así que no puede ser usado para los fines previstos.	No	**si (Accidentalmente)**	si (intencionalmente)

Escenario2: Pensar en personas que son externas a la Institución. Esto podría personas quienes tienen una relación de negocio con la Institución o no. ¿Hay alguna situación en la cual un externo, accidental o intencionalmente, podría causar que el activo de información sea:			
Divulgado a personas no autorizadas?	**No**	si (Accidentalmente)	si (intencionalmente)

Tabla 23 Octave-Allegro Cuestionario #2

Escenario3: Considerar situaciones que podrían afectar el activo de información en cualquier contenedor técnico identificado. Determinar si cualquiera de las siguientes situaciones podría ocurrir, y si es afirmativo, determinar si estas situaciones podrían causar uno o más de los siguientes resultados.					
· La divulgación no intencional del activo de información. · La modificación no intencional del activo de información. · La interrupción no intencional de la disponibilidad del activo de información. · La destrucción permanente o temporal no intencional del activo de información.					
Un defecto de software.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Un fallo del sistema de origen conocido o desconocido.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Un defecto de hardware.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Código malicioso (virus, gusanos, Caballo de Troya, o puerta trasera) es ejecutado.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Fuente de energía de los contenedores es interrumpida	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Problemas con las telecomunicaciones.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Otros problemas de terceros o Sistemas.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Desastres naturales o causados por el hombre.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)

Tabla 24 Octave-Allegro Cuestionario #1

Cuestionario1 - SISTEMA DE BODEGA	**Contenedores Técnicos**		
Escenario1: Pensar acerca de las personas que trabajan en la Institución. ¿Hay una situación en la que un empleado podría acceder a uno o más contenedores técnicos, accidentalmente o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?	**No**	si (Accidentalmente)	si (intencionalmente)
Modificado así que no sea utilizable para los fines previstos?	No	**si (Accidentalmente)**	si (intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?	No	**si (Accidentalmente)**	si (intencionalmente)
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?	No	**si (Accidentalmente)**	**si (intencionalmente)**
Escenario2: Pensar en personas que son externas a la Institución. Podría incluir a personas que tienen relación de negocio con la Institución o no. ¿ Hay alguna situación en la cual un externo podría acceder uno o más contenedores técnicos, accidental o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?	**No**	si (Accidentalmente)	Si (intencionalmente)
Modificado así que no sea utilizable para los fines previstos?	**No**	si (Accidentalmente)	si (intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?	No	**si (Accidentalmente)**	**si (intencionalmente)**
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?	**No**	si (Accidentalmente)	si (intencionalmente)

Tabla 25 Octave-Allegro Cuestionario #2

Cuestionario2	**Contenedores Técnicos**		
Escenario1: Pensar en las personas que trabajan en la Institución. ¿Hay una situación en la cual un empleado tiene conocimiento detallado de su activo de información y podría, accidental o intencionalmente, causar que el activo de información sea:			
Divulgado a personas no autorizadas?	**No**	si (Accidentalmente)	si (intencionalmente)
Modificado, de tal manera que no sea utilizable para los fines previstos.	No	**si (Accidentalmente)**	**si (intencionalmente)**
Interrumpido, así que no puede ser accedido para los fines previstos.	No	**si (Accidentalmente)**	si (intencionalmente)
Permanentemente destruido o temporalmente perdido, así que no puede ser usado para los fines previstos.	No	**si (Accidentalmente)**	si (intencionalmente)
Escenario2: Pensar en personas que son externas a la Institución. Esto podría personas quienes tienen una relación de negocio con la Institución o no. ¿Hay alguna situación en la cual un externo, accidental o intencionalmente, podría causar que el activo de información sea:			
Divulgado a personas no autorizadas?	**No**	si (Accidentalmente)	si (intencionalmente)

Tabla 26 Octave-Allegro Cuestionario #2

Escenario3: Considerar situaciones que podrían afectar el activo de información en cualquier contenedor técnico identificado. Determinar si cualquiera de las siguientes situaciones podría ocurrir, y si es afirmativo, determinar si estas situaciones podrían causar uno o más de los siguientes resultados. · La divulgación no intencional del activo de información. · La modificación no intencional del activo de información. · La interrupción no intencional de la disponibilidad del activo de información. · La destrucción permanente o temporal no intencional del activo de información.					
Un defecto de software.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Un fallo del sistema de origen conocido o desconocido.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Un defecto de hardware.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Código malicioso (virus, gusanos, Caballo de Troya, o puerta trasera) es ejecutado.	No	si (Divulgación)	**Si (modificación)**	**si (Interrupción)**	Si (perdida)
Fuente de energía de los contenedores es interrumpida	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Problemas con las telecomunicaciones.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Otros problemas de terceros o Sistemas.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)
Desastres naturales o causados por el hombre.	No	si (Divulgación)	Si (modificación)	**si (Interrupción)**	Si (perdida)

4.7 IDENTIFICAR ÁREAS DE INTERÉS Y RIESGOS DEL ACTIVO DE INFORMACIÓN

Para este paso se utiliza la plantilla 10 de Octave-Allegro. En esta plantilla se maneja la información correspondiente al riesgo del activo de información y se da la descripción de cómo debe ser llenada en sus diferentes campos.

Un área de preocupación es una declaración descriptiva que detalla una condición o situación del mundo real que pueda afectar al activo de información. De acuerdo al área de preocupación definida las consecuencias y la probabilidad de ocurrencia irán variando.

La sección de amenaza se compone de campos como, el área de preocupación, en el cual se manejan campos como el actor que es quien podría causar problema al sistema, el medio que se utilizaría para explotar la vulnerabilidad.

La motivación puede ser accidental o intencional, la consecuencia es lo que podría resultar de afectar al activo de información, los requerimientos de

seguridad que podrían acortar la brecha y la probabilidad que este escenario de amenaza ocurra.

El campo severidad se conforma de las áreas de impacto seleccionadas se toma en cuenta de 1 a 3 siendo 1 el más bajo y 3 el más alto.

El campo valor se deriva de la escala seleccionada para cada área de impacto, la cual es alta, media y baja, para realizar el cálculo de la puntuación del riesgo estos niveles se traducen a números es decir alta=3, media=2, baja=1.

Al final se suma la columna de la puntuación para obtener el valor de riesgo en las áreas de interés con la amenaza analizada.

Tabla 27 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al sistema de ventas		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso a la PC		
		Probabilidad	Alta	**media**	baja
	Consecuencia generar ventas no solicitadas		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alto	6
			Productividad	Medio	2

Tabla 28 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al sistema de ventas		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso a la PC		
		Probabilidad	alta	**media**	baja
	Consecuencia información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 29 Octave-Allegro Hoja de Trabajo #10

	Riesgo del Activo de Información				
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Que un empleado haga uso de un usuario y clave de otro empleado para ingresar al sistema		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Borrar información		
		Consecuencia	Divulgación	Modificación	**Destrucción** Interrupción
		Requerimiento de Seguridad	Tener un log de cambios realizados por los usuarios		
		Probabilidad	alta	**media**	baja
	Consecuencia modificar o eliminar información		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alta	6
			Productividad	Alta	3

Tabla 30 Octave-Allegro Hoja de Trabajo #10

	Riesgo del Activo de Información				
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Usuarios externos puedan tener acceso al sistema (hackers)		
		Actor	Hackers		
		Medio	Acceso vía Web		
		Motivo	Causar daño a la reputación de la empresa		
		Consecuencia	**Divulgación**	**Modificación**	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso a través de la red externa		
		Probabilidad	alta	**media**	baja
	Consecuencia Robo o modificación de información sensible		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alto	6
			Productividad	Alto	3

Tabla 31 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Al momento de actualizar el sistema los cambios realizados no permiten al sistema funcionar correctamente		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Generar una política de control de cambios		
		Probabilidad	**alta**	media	baja
	Consecuencia la empresa no podría vender		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alto	6
			Productividad	Media	2

Tabla 32 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Alguna Persona de DS que quiera causar daño a la empresa		
		Actor	Empleado		
		Medio	PC, vía remota		
		Motivo	Robar información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Crear políticas de Control de Acceso		
		Probabilidad	**alta**	**media**	baja
	Consecuencia información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alto	3

Tabla 33 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al sistema de ventas		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso a la		
		Probabilidad	alta	**media**	baja
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 34 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Un empleado es despedido y no devuelve la laptop que está a su cargo		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener una política para la devolución de equipos		
		Probabilidad	alta	media	**baja**
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 35 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Falla en el Router del proveedor		
		Actor	CNT		
		Medio	Router		
		Motivo	Falla		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Realizar monitoreas o tener un proveedor de respaldo		
		Probabilidad	alta	**media**	baja
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 36 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Empleado de TI realiza pruebas en producción		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Control de acceso y separación de los ambientes de prueba y producción		
		Probabilidad	**alta**	media	Baja
	Consecuencia podría causar interrupción del sistema		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alto	6
			Productividad	Medio	2

Tabla 37 Octave-Allegro Hoja de Trabajo #10

	Riesgo del Activo de Información				
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Personal externo solicita acceso al servidor de pruebas y obtiene acceso a los datos del servidor de pruebas		
		Actor	Proveedor		
		Medio	Acceso desde PC / laptop		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Destrucción de los datos de prueba en ambientes de desarrollo		
		Probabilidad	alta	**media**	baja
	Consecuencia la información podría ser utilizada para acceder al sistema y causar interrupción		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Medio	6
			Productividad	Medio	2

Tabla 38 Octave-Allegro Hoja de Trabajo #10

	Riesgo del Activo de Información				
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Empleado instala software sin autorización		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Por diversión para poder escuchar música		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Manejar un control de acceso según perfil		
		Probabilidad	alta	**media**	baja
	Consecuencia la información podría ser utilizada para causar interrupción		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Medio	2

}

Tabla 39 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	El acceso al sistema maneja un pin de 5 dígitos numéricos. Lo que hace muy probable averiguar el pin de acceso		
		Actor	Cualquiera		
		Medio	Acceso desde PC / laptop		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Definir reglas para la creación de clave segura		
		Probabilidad	alta	**media**	baja
	Consecuencia la información ser divulgada o modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 40 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Se evidencian registros realizados con códigos de empleado que ya no trabajan en la empresa		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	Divulgación	**Modificación**	Destrucción Interrupción
		Requerimiento de Seguridad	Educar al usuario sobre el uso y la confidencialidad de las claves		
		Probabilidad	**alta**	media	baja
	Consecuencia la información podría ser modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alto	3

Tabla 41 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Ventas		
		Área de Preocupación	Ex Empleado puede buscar lucrar con la información que conoce o que manejaba		
		Actor	Empleado Enojado		
		Medio	Vía Red		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Acuerdo de Confidencialidad		
		Probabilidad	alta	media	**baja**
	Consecuencia la información ser divulgada o modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alta	6
			Productividad	Media	2

Tabla 42 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al Sistema Interno		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso a la		
		Probabilidad	alta	**media**	baja
	Consecuencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
	generar ventas no solicitadas por los clientes		Reputación	Medio	4
			Productividad	Medio	2

Tabla 43 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al Sistema Interno		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso a la		
		Probabilidad	alta	**media**	baja
	Consecuencia La información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 44 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Que un empleado haga uso de un usuario y clave de otro empleado para ingresar al sistema		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Borrar información		
		Consecuencia	Divulgación	Modificación	**Destrucción** Interrupción
		Requerimiento de Seguridad	Tener un log de cambios realizados por los usuarios		
		Probabilidad	alta	**media**	baja
	Consecuencia el usuario podría modificar o eliminar información		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Medio	4
			Productividad	Alta	3

Tabla 45 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Usuarios externos puedan tener acceso al sistema (hackers)		
		Actor	Hackers		
		Medio	Acceso vía Web		
		Motivo	Causar daño a la reputación de la empresa		
		Consecuencia	**Divulgación**	**Modificación**	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso al sistema		
		Probabilidad	alta	**media**	baja
	Consecuencia Robo o modificación de información sensible para el negocio		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Medio	4
			Productividad	Alto	3

Tabla 46 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Al momento de actualizar el sistema los cambios realizados no permiten al sistema funcionar correctamente		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Generar una política de control de cambios		
		Probabilidad	**alta**	media	baja
	Consecuencia La empresa no podría vender		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alto	2

Tabla 47 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Alguna Persona de DS que quiera causar daño a la empresa		
		Actor	Empleado		
		Medio	PC, vía remota		
		Motivo	Robar información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Crear políticas de Control de Acceso		
		Probabilidad	**alta**	**media**	baja
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alto	3

Tabla 48 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al Sistema Interno		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Sistema Interno		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso		
		Probabilidad	**alta**	**media**	baja
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alto	3

Tabla 49 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Un empleado es despedido y no devuelve la laptop que está a su cargo		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener una política para la devolución de equipos		
		Probabilidad	alta	media	**baja**
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 50 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Falla en la replicación de las bases locales para vendedores		
		Actor	Servidor Replicador		
		Medio	Red		
		Motivo	Falla		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Realizar monitoreo		
		Probabilidad	alta	**media**	baja
	Consecuencia el vendedor no contaría con la información		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alto	6
			Productividad	Alto	3

Tabla 51 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Empleado de TI realiza pruebas en producción		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Control de acceso y separación de los ambientes de prueba y producción		
		Probabilidad	**alta**	media	Baja
	Consecuencia Se pierde la confianza en el DS		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	6
			Productividad	Medio	2

Tabla 52 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Personal externo solicita acceso al servidor de pruebas y obtiene acceso a los datos del servidor de pruebas		
		Actor	Proveedor		
		Medio	Acceso desde PC / laptop		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Destrucción de los datos de prueba en ambientes de desarrollo		
		Probabilidad	alta	**media**	baja
	Consecuencia la información podría ser utilizada para causar interrupción		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Medio	6
			Productividad	Medio	2

Tabla 53 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Empleado instala software sin autorización		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Por diversión para poder escuchar música		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Manejar un control de acceso según perfil		
		Probabilidad	alta	**media**	baja
	Consecuencia la información podría ser utilizada para causar interrupción		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Medio	2

Tabla 54 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	El acceso al sistema maneja un pin de 5 dígitos numéricos. Lo que hace muy probable averiguar el pin de acceso		
		Actor	Cualquiera		
		Medio	Acceso desde PC / laptop		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Definir reglas para la creación de clave segura		
		Probabilidad	alta	**media**	baja
	Consecuencia la información ser divulgada o modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 55 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Se evidencian registros realizados con códigos de empleado que ya no trabajan en la empresa		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	Divulgación	**Modificación**	Destrucción Interrupción
		Requerimiento de Seguridad	Educar al usuario sobre el uso y la confidencialidad de las claves		
		Probabilidad	**alta**	media	baja
	Consecuencia la información podría ser modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alto	3

Tabla 56 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Ex Empleado puede buscar lucrar con la información que conoce o que manejaba		
		Actor	Empleado Enojado		
		Medio	Vía Red		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Acuerdo de Confidencialidad		
		Probabilidad	alta	media	**baja**
	Consecuencia la información ser divulgada o modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alta	6
			Productividad	Media	2

Tabla 57 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema Interno		
		Área de Preocupación	Empleado puede llamar al sistema interno utilizando línea de comandos		
		Actor	Empleado		
		Medio	PC / Laptop		
		Motivo	Intencional		
		Consecuencia	Divulgación	**Modificación**	Destrucción Interrupción
		Requerimiento de Seguridad	Control de desarrollo de software seguro que solicite autenticación por usuario y clave en toda llamada al sistema		
		Probabilidad	alta	media	**baja**
	Consecuencia la información ser divulgada o modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Media	4
			Productividad	Alta	3

Tabla 58 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al Sistema de Bodega		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso a la		
		Probabilidad	alta	media	baja
	Consecuencia se podría generar ventas no solicitadas por los clientes		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Medio	4
			Productividad	Alta	3

Tabla 59 Octave-Allegro Hoja de Trabajo #10

	Riesgo del Activo de Información				
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al Sistema de Bodega		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso		
		Probabilidad	alta	**media**	Baja
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alta	3

Tabla 60 Octave-Allegro Hoja de Trabajo #10

	Riesgo del Activo de Información				
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Que un empleado haga uso de un usuario y clave de otro empleado para ingresar al sistema		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Borrar información		
		Consecuencia	Divulgación	Modificación	**Destrucción** Interrupción
		Requerimiento de Seguridad	Tener un log de cambios realizados por los usuarios		
		Probabilidad	alta	**media**	baja
	Consecuencia el usuario podría modificar o eliminar información		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Medio	4
			Productividad	Alta	3

Tabla 61 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Usuarios externos puedan tener acceso al sistema (hackers)		
		Actor	Hackers		
		Medio	Acceso vía Web		
		Motivo	Causar daño a la reputación de la empresa		
		Consecuencia	**Divulgación**	**Modificación**	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso al sistema		
		Probabilidad	alta	**media**	baja
	Consecuencia se podría dar el Robo o modificación de información sensible		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Medio	4
			Productividad	Alto	3

Tabla 62 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	Riesgo	Riesgo		
		Área de Preocupación	Al momento de actualizar el sistema los cambios realizados no permiten al sistema funcionar correctamente		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Generar una política de control de cambios		
		Probabilidad	**alta**	media	Baja
	Consecuencia Si este escenario ocurriera la empresa no podría vender		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alto	6
			Productividad	Alto	2

Tabla 63 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Alguna Persona de DS que quiera causar daño a la empresa		
		Actor	Empleado		
		Medio	PC, vía remota		
		Motivo	Robar información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Crear políticas de Control de Acceso		
		Probabilidad	**alta**	**media**	Baja
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alto	3

Tabla 64 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Que un empleado haga uso de una PC que no está a su cargo para acceder al Sistema de Bodega		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener un control de acceso		
		Probabilidad	alta	**media**	baja
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 65 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Un empleado es despedido y no devuelve la laptop que está a su cargo		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Quiere obtener beneficio de la información		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Tener una política para la devolución de equipos		
		Probabilidad	alta	media	**baja**
	Consecuencia la información podría llegar a la competencia		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 66 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Empleado de TI realiza pruebas en producción		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Control de acceso y separación de los ambientes de prueba y producción		
		Probabilidad	**alta**	media	Baja
	Consecuencia se pierde la confianza en el DS		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	6
			Productividad	Alto	3

Tabla 67 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Personal externo solicita acceso al servidor de pruebas y obtiene acceso a los datos del servidor de pruebas		
		Actor	Proveedor		
		Medio	Acceso desde PC / laptop		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Destrucción de los datos de prueba en ambientes de desarrollo		
		Probabilidad	alta	**media**	Baja
	Consecuencia la información podría ser utilizada para causar interrupción		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Medio	6
			Productividad	Bajo	2

Tabla 68 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Empleado instala software sin autorización		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Por diversión para poder escuchar música		
		Consecuencia	Divulgación	Modificación	Destrucción **Interrupción**
		Requerimiento de Seguridad	Manejar un control de acceso según perfil		
		Probabilidad	alta	**media**	baja
	Consecuencia la información podría ser utilizada para causar interrupción		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Medio	2

Tabla 69 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	El acceso al sistema maneja un pin de 5 dígitos numéricos. Lo que hace muy probable averiguar el pin de acceso		
		Actor	Cualquiera		
		Medio	Acceso desde PC / laptop		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Definir reglas para la creación de clave segura		
		Probabilidad	alta	**media**	baja
	Consecuencia la información ser divulgada o modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Bajo	1

Tabla 70 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Se evidencian registros realizados con códigos de empleado que ya no trabajan en la empresa		
		Actor	Empleado		
		Medio	Acceso desde PC / laptop		
		Motivo	Accidental		
		Consecuencia	Divulgación	**Modificación**	Destrucción Interrupción
		Requerimiento de Seguridad	Educar al usuario sobre el uso y la confidencialidad de las claves		
		Probabilidad	**alta**	media	baja
	Consecuencia Si este escenario ocurriera la información podría ser modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Bajo	3
			Productividad	Alto	3

Tabla 71 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de información	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Ex Empleado puede buscar lucrar con la información que conoce o que manejaba		
		Actor	Empleado Enojado		
		Medio	Vía Red		
		Motivo	Intencional		
		Consecuencia	**Divulgación**	Modificación	Destrucción Interrupción
		Requerimiento de Seguridad	Acuerdo de Confidencialidad		
		Probabilidad	alta	Media	**baja**
	Consecuencia la información ser divulgada o modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Alta	6
			Productividad	Baja	2

Tabla 72 Octave-Allegro Hoja de Trabajo #10

		Riesgo del Activo de Información			
Riesgo del activo de nformación	Amenaza	**Activo de Información**	Sistema de Bodega		
		Área de Preocupación	Empleado puede llamar al Sistema de Bodega utilizando línea de comandos		
		Actor	Empleado		
		Medio	PC / Laptop		
		Motivo	Intencional		
		Consecuencia	Divulgación	**Modificación**	Destrucción Interrupción
		Requerimiento de Seguridad	Control de desarrollo de software seguro que solicite autenticación por usuario y clave en toda llamada al sistema		
		Probabilidad	alta	media	**baja**
	Consecuencia la información ser divulgada o modificada		**Severidad**		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación	Media	4
			Productividad	Alta	3

4.8 ANÁLISIS DE RIESGOS Y SELECCIÓN DE MITIGACIÓN

Se utiliza el método de categorización realizado en Octave-Allegro que indica que se debe clasificar los riesgos de mayor a menor y agruparlos en rangos de riesgos.

Tabla 73 Matriz de riesgo

Probabilidad	**Puntaje de Riesgo**		
	7 - 9	**4 - 6**	**1- 3**
Alto	rango 1	rango 2	rango 3
Medio	rango 2	rango 3	rango 4
Bajo	rango 3	rango 4	Rango 4

Tabla 74 Tabla de rangos y mitigación

Rango	**Tipo de Mitigación**
Rango 1	Mitigarlo
Rango 2	Mitigarlo o Aplazarlo
Rango 3	Aplazarlo o Aceptarlo
Rango 4	Aceptarlo

Se tabula las repuestas afirmativas de cada cuestionario y se realiza una referencia cruzada con cada escenario de posibles amenazas descritas en la sección anterior con sus respectivas consecuencias. Además se agrega el valor de la suma de la columna puntuación de cada posible

amenaza. Además se incorpora las la columna de prioridad de mitigación por área de impacto.

Tabla 75 Posición del riesgo y prioridad de mitigación

Escenario	Consecuencia	Posición del riesgo	Prioridad de Mitigación	Control
Que un empleado haga uso de una PC que no está a su cargo para acceder a los diferentes Sistemas	Si este escenario ocurriera se podría generar ventas no solicitadas por los clientes	8	2	8.1.3
Que un empleado haga uso de un usuario y clave de otro empleado para ingresar al sistema	Si este escenario ocurriera el usuario podría modificar o eliminar información	9	2	9.2.1 9.3.1
Usuarios externos puedan tener acceso al sistema (hackers)	Si este escenario ocurriera se podría dar el Robo o modificación de información sensible para el negocio	7	2	9.1.2
Al momento de actualizar el sistema los cambios realizados no permiten al sistema funcionar correctamente	Si este escenario ocurriera la empresa no podría vender	8	1	14.2.5 14.2.8

Tabla 76 Posición del riesgo y prioridad de mitigación

Escenario	Consecuencia	Posición del riesgo	Prioridad de Mitigación	Control
Alguna Persona de DS que quiera causar daño a la empresa	Si este escenario ocurriera la información podría llegar a la competencia	6	2	
Un empleado es despedido y no devuelve la laptop que está a su cargo	Si este escenario ocurriera la información podría llegar a la competencia	4	3	8.1.4 8.1.1
Empleado de TI realiza pruebas en producción	Si este escenario ocurriera podría causar interrupción del sistema	8	2	9.4.1
Personal externo solicita acceso al servidor de pruebas y obtiene acceso a los datos del servidor de pruebas	Si este escenario ocurriera podría causar interrupción del sistema	8	3	9.1.2 9.4.1 14.2.8
Empleado instala software sin autorización	Si este escenario ocurriera la información podría ser utilizada para acceder al sistema y causar interrupción	5	3	9.2.3
El acceso al sistema maneja un pin de 5 dígitos numéricos.	Si este escenario ocurriera la información ser divulgada o modificada	4	3	9.4.3
Se evidencian registros realizados con códigos de empleado que ya no trabajan en la empresa	Si este escenario ocurriera la información podría ser modificada	6	2	9.2.1, 9.2.6
Falla en la replicación de las bases locales para vendedores	Si este escenario ocurriera el vendedor no contaría con la información actualizada	9	1	13.2.1
Empleado puede llamar al sistema interno utilizando línea de comandos	Si este escenario ocurriera la información ser divulgada o modificada	7	3	9.4.1

4.9 DISEÑO DE LA POLITICA

Luego de haber realizado el análisis con la ayuda de las plantillas de la metodología seleccionada se procede con el diseño de la política

Objetivo

Proteger ante amenaza, interna o externa, que pudieran poner en riesgo la confidencialidad, integridad y disponibilidad de la información de la organización mediante el uso de las Políticas de Seguridad de la Información.

Alcance

Se definirá políticas en base a los controles definidos en la norma ISO/IEC 27002. La política se extenderá a todo los usuarios que hagan uso de los Sistemas interno, de logística y de ventas.

Roles y responsabilidades

Áreas Involucradas Debe existir la coordinación de todos los departamentos involucrados para que la política se pueda implementar y sea sustentable en el tiempo.

Empleados, responsables de cumplimiento de las políticas

Gerencia de Sistemas, encargada de la administración de las políticas.

Cumplimiento

Para el cumplimiento de la política se ha definido el rol de oficial de seguridad de la información, esta persona se encargara del control y monitoreo de las misma.

POLÍTICA GENERAL

Objetivo:

El objetivo de la política general es el de establecer una gestión adecuada de la seguridad de la información basada en las políticas específicas definidas.

Aplicación:

La política general de seguridad de la información, será obligatoria para todos los empleados y terceros que tengan acceso a la información de la empresa.

Sanciones:

El incumplimiento de la política estará sujeto a investigación por parte de la administración y de ser necesario a las sanciones disciplinarias previstas por el departamento de Recursos Humanos.

Actualización:

La política será revisada semestralmente por el oficial de seguridad y los cambios propuestos serán revisados por el comité de seguridad de la información y aprobados por la gerencia.

Difusión:

La difusión de la Política estará a cargo del Oficial de Seguridad en coordinación con el departamento de comunicación.

POLÍTICA DE CONTROL DEL ACCESO

Objetivo:

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

1. Para la asignación de accesos a los diferentes sistemas el usuario deberá realizar la solicitud indicando el nombre del

sistema, y esta solicitud será devuelva con el nombre del usuario, contraseña temporal y los permisos asignados.

2. La contraseña estará compuesta de 8 caracteres alfanuméricos y al menos deberá tener un número, una letra mayúscula.
3. La contraseña tendrá un periodo de vigencia de 2 meses
4. El usuario se bloqueara luego del 3 intento de acceso fallido.
5. La nueva contraseña no podrá ser igual a las 5 últimas ingresadas
6. Los usuarios y contraseñas son personales e intransferibles.
7. No compartir las contraseñas, con otros usuarios.
8. Si tiene conocimiento o sospecha de que alguien conoce su contraseña, cámbiela inmediatamente.
9. El acceso a la red a través de los puertos, estarán basadas en la premisa “todo está restringido, a menos que este expresamente permitido“.
10. Controlar el acceso a los servicios de red tanto internos como externos.
11. Identificar las redes y servicios de red a los cuales se permite el acceso.
12. La instalación de cualquier tipo de software será permitido solo a los usuarios administradores, bajo ningún concepto un

usuario final podrá tener permisos para la instalación de software no autorizados.

13. Para el caso de los dispositivos móviles se establecerán los siguientes:
14. Es obligatorio el uso de usuario y contraseña para acceso al mismo.
15. Cifrado de la información.
16. Uso de software antivirus
17. Permanecer siempre cerca del dispositivo
18. No conectarse a redes inalámbricas públicas

POLITICA DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Objetivo:

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

1. Durante la etapa de diseño de un software se deberá considerar lo siguiente:
    - 1.1 Control de secuencia por cada desarrollo
    - 1.2 Control de acceso por tipo de usuario.
    - 1.3 Control de los valores de ingreso al sistema

1.4 Control de los valores cargados en las tablas de datos.

2. Validar los datos de salida con el fin de garantizar la ejecución correcta según los requerimientos funcionales del proyecto.
3. Los datos de pruebas deberán ser protegidos por lo cual se deberá:

3.1 Solicitar autorización para realizar una copia de la base de datos que se requiere y colocarla en un ambiente de prueba.

3.2 Luego de terminadas las pruebas la base de prueba debe ser eliminada.

3.3 Los datos en ambiente de prueba se mantendrán vigentes por un periodo de dos meses.

4. El acceso a los códigos fuente deberá considerar lo siguiente:

4.1 Proveer al Área de Desarrollo los programas fuente solicitados mediante una solicitud formal

4.2 Llevar un registro de todos los programas fuente, indicando su estado así como el nombre del programa, versión, fecha de última modificación y fecha del ejecutable.

4.3 Solo el custodio tendrá acceso a los ambientes y a las herramientas que permitan la manipulación de los programas fuente.

5. Verificar que los cambios sean propuestos por usuarios autorizados.
6. Solicitar la autorización del propietario de la Información, en caso de tratarse de cambios que afecten varias partes del sistema.
7. Solicitar la revisión del Oficial de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
8. Mantener un control de versiones para todas las actualizaciones.

POLITICA DE MANEJO DE ACTIVOS

Objetivo:

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos

1. Se mantendrá un inventario actualizado de los activos de información, el cual contara con el nombre del responsable del activo de información.
2. Los usuarios deberán utilizar únicamente los programas y equipos asignados.

3. Se proporcionará al usuario los equipos informáticos y estos estarán ya completamente configurados y con los software instalados en ellos. Los datos o información creados, almacenados y recibidos, serán propiedad de la organización.
4. Los usuarios que requieran realizar copias de cualquier tipo de información clasificada o reservada deberán pedir autorización a su jefe inmediato con copia al DS para que se pueda gestionar el requerimiento.
5. Cualquier copia, sustracción, daño intencional o utilización incorrecta de alguno de los activos será sujeto de sanción la misma que será determinada por la gerencia de la organización luego de informe presentado por el DS.
6. Periódicamente, el DS efectuará la revisión de los programas utilizados en cada activo asignado al usuario.
7. Estarán bajo custodia del Área DS los medios magnéticos/electrónicos (disquetes, Cd u otros) software con sus respectivos manuales y licencias.
8. El oficial de seguridad con autorización de la gerencia del DS podrá acceder a revisar cualquier tipo de activo de información así como la información que es enviada o descargada desde el internet o vía correo electrónico.

9. Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos a ellos asignados.

CAPÍTULO 5

IMPLEMETACIÓN DE LA POLITICA DE SEGURIDAD

5.1 PLAN DE IMPLEMENTACIÓN

Para la asignación de accesos a los diferentes sistemas se ha optado por la creación de la Solicitud de Acceso la cual es un documento mediante el cual el usuario y jefe del área solicitan permisos para acceder al sistema que indiquen. La misma se encuentra en el anexo B.

Con esto se quiere lograr tener un control de los permisos que se otorgan a cada usuario.

La implementación de clave segura se llevara en 3 etapas, primero el análisis del sistema en donde se debe implementar segundo el cambio propiamente solicitado y por último la difusión.

El acceso a los sistemas anteriormente expuestos es de acceso único, solo se debe colocar usuario y contraseña y el sistema al que se desee acceder. Estos cambios implican:

1.- Expandir la cantidad máxima de dígitos a guardar en base

2.- Modificar el programa de acceso para incluir las restricciones expuestas en los puntos 2, 3, 4,5 de la política de control de accesos.

3.- Finalmente, todas las contraseñas serán restauradas para que el que al primer inicio de acceso el usuario ingrese una nueva clave que ya considera las nuevas políticas.

Para el desarrollo se ha considerado un tiempo de 4 semanas luego de lo cual se procederá con la difusión para finalmente la implementación.

Tabla 77 Cronograma de desarrollo para implementación de clave segura

Tarea	Recursos	Días
Análisis	1	3
Creación Nuevas Estructuras	1	3
Modificación de Aplicaciones	3	3
Restauración de Claves	1	1
Pruebas Internas	3	1
Capacitación	3	3
Pruebas Control Calidad	1	3
Pruebas con Usuarios	1	3
Implementación	2	1
Difusión	1	1

El cronograma propuesto se desarrollara con un total de 5 recursos distribuidos en analisis (1) , creacion de estructuras (1) y para el resto de tareas (3).

Figura 5.1 Línea de Tiempo de Desarrollo

Para lo referente al punto 9, 10, 11, 12 se realizaron varias reuniones con el personal de infraestructura quienes son los encargados de aplicar las políticas descritas. Para lo cual solicitaron como plazo 2 semanas.

Adicionalmente, se revalidaran todos los accesos de los usuarios para asegurarse que solo los usuarios designados tengan permisos de administrador y existe una adecuada segregación de funciones.

Para el caso de las personas que utilizan dispositivos móviles se indicara la política en el capítulo de difusión.

Como parte de la implementación de la política de desarrollo y mantenimiento de sistemas se han establecido plantillas que deberán ser utilizadas para:

1. Solicitud de Modificación del Fuente
2. Pruebas de la Aplicación en Etapa de Desarrollo
3. Pruebas de la Aplicación con el Usuario Final
4. Registro de Cambios realizados al Fuente

Finalmente, para la política de manejo de activos, se realizó fue la aprobación formal ya que la misma era utilizada a forma de guía por parte del personal del departamento. Esta política será difundida en el departamento para conocimiento de todos.

5.2 PLAN DE PRUEBAS

Luego de realizados los cambios, se procede a realizar las pruebas tanto con el departamento de desarrollo como con apoyo de los catálogos que se encuentran en el anexo B.

5.3 DIFUSIÓN DE LA POLÍTICA

La última fase es la difusión de la política, cuyo objetivo es que el personal del departamento y la empresa tomen conciencia de las políticas y adquieran una cultura de seguridad. Dentro de la difusión se enfoca los objetivos de la política y como nos ayudan a realizar de forma segura nuestras actividades.

Las estrategias utilizadas

1. Charlas a todo el personal
2. Entrega de la política de forma impresa
3. Evaluaciones periódicas sobre la política

4. Juegos interactivos periódicos en base a preguntas sobre las políticas a modo de concurso.

CAPÍTULO 6

ANALISIS DE RESULTADOS

6.1 EVALUAR SI LAS AMENAZAS PRESENTADAS EN LA MATRIZ DE RIESGO FUERON MITIGADAS.

Luego de implementada la política se realizó una nueva evaluación para determinar si la política ha sido de ayuda para mitigar los problemas encontrados a través de los escenarios planteados. En la siguiente tabla se indica la posición del riesgo detectada y se compara junto a la del riesgo residual.

Tabla 78 Tabla de análisis de riesgo residual

Escenario	Consecuencia	Posición del riesgo	Posición del riesgo Residual
Que un empleado haga uso de una PC que no está a su cargo para acceder a los diferentes Sistemas	Si este escenario ocurriera se podría generar ventas no solicitadas por los clientes	Rango 2 Mitigar	Rango 4
Que un empleado haga uso de un usuario y clave de otro empleado para ingresar al sistema	Si este escenario ocurriera el usuario podría modificar o eliminar información	Rango 1 Mitigar	Rango 4
Usuarios externos puedan tener acceso al sistema (hackers)	Si este escenario ocurriera se podría dar el Robo o modificación de información sensible para el negocio	Rango 3 Aplazar	Rango 3
Al momento de actualizar el sistema los cambios realizados no permiten al sistema funcionar correctamente	Si este escenario ocurriera la empresa no podría vender	Rango 2 Mitigar	Rango 4
Alguna Persona de DS que quiera causar daño a la empresa	Si este escenario ocurriera la información podría llegar a la competencia	Rango 2 Aplazar	Rango 4
Un empleado es despedido y no devuelve la laptop que está a su cargo	Si este escenario ocurriera la información podría llegar a la competencia	Rango 4 Aceptar	Rango 4
Empleado de TI realiza pruebas en producción	Si este escenario ocurriera podría causar interrupción del sistema	Rango 2 Mitigar	Mitigado
Personal externo solicita acceso al servidor de pruebas y obtiene acceso a los datos del servidor de pruebas	Si este escenario ocurriera podría causar interrupción del sistema	Rango 2 Mitigar	Mitigado
Empleado instala software sin autorización	Si este escenario ocurriera la información podría ser utilizada para acceder al sistema y causar interrupción	Rango 3 Aplazar	Mitigado
El acceso al sistema maneja un pin de 5 dígitos numéricos. Lo que hace muy probable averiguar el pin de acceso	Si este escenario ocurriera la información ser divulgada o modificada	Rango 4 Aplazar	Mitigado

Tabla 79 Tabla de análisis de riesgo residual

Escenario	Consecuencia	Posición del riesgo	Posición del riesgo Residual
Se evidencian registros realizados con códigos de empleado que ya no trabajan en la empresa	Si este escenario ocurriera la información podría ser modificada	Rango 2 Mitigar	Mitigado
Falla en la replicación de las bases locales para vendedores	Si este escenario ocurriera el vendedor no contaría con la información actualizada	Rango 1 Mitigar	Aplazar
Empleado puede llamar al sistema interno utilizando línea de comandos	Si este escenario ocurriera la información ser divulgada o modificada	Rango 3 Aplazar	Rango 4

Aunque la mayoría de los riesgos fueron mitigados existen otros que fueron aplazados, aunque la metodología utiliza la palabra aplazar se determinó que lo mejor sería indicar transferir, ya que es la mejor forma de mitigar estos riesgos.

6.2 ANALIZAR LOS RIEGOS QUE SE MANTUVIERAN, A PESAR QUE LAS VULNERABILIDADES FUERON MITIGADAS.

Los riesgos que se presentan a continuación se considera que a pesar de las medidas tomadas aún se encuentran presentes, ya que es posible que alguno de estos escenarios se presente. Las medidas tomadas ayudaron a disminuir la probabilidad de que el riesgo ocurra, sin embargo, se considera que los mismos siempre estarán presentes aunque con menor posibilidad.

Tabla 80 Tabla de análisis de riesgo mantenidos

Escenario	Consecuencia	Posición del riesgo	Posición del riesgo Residual
Que un empleado haga uso de una PC que no está a su cargo para acceder a los diferentes Sistemas	Si este escenario ocurriera se podría generar ventas no solicitadas por los clientes	Rango 2 Mitigar	Rango 4
Que un empleado haga uso de un usuario y clave de otro empleado para ingresar al sistema	Si este escenario ocurriera el usuario podría modificar o eliminar información	Rango 1 Mitigar	Rango 4
Al momento de actualizar el sistema los cambios realizados no permiten al sistema funcionar correctamente	Si este escenario ocurriera la empresa no podría vender	Rango 2 Mitigar	Rango 4
Alguna Persona de DS que quiera causar daño a la empresa	Si este escenario ocurriera la información podría llegar a la competencia	Rango 2 Aplazar	Rango 4
Un empleado es despedido y no devuelve la laptop que está a su cargo	Si este escenario ocurriera la información podría llegar a la competencia	Rango 4 Aceptar	Rango 4

6.3 IMPACTO EN LA GESTIÓN ADMINISTRATIVA, QUE GENERA LA IMPLEMENTACIÓN DE LAS NUEVAS POLÍTICAS DE SEGURIDAD.

Luego de la implementación y difusión de las políticas se ha podido evidenciar una disminución en los incidentes reportados por parte de los usuarios en lo referente a errores reportados por transacciones realizadas con usuarios inexistentes o de usuarios que aseguran no ha ver realizado transacciones por las cuales solicitan revisiones. En el periodo de Octubre a Diciembre de 2016 se pudo constatar que se han eliminado completamente los errores reportados por fallos de ejecuciones en producción.

Los tiempos para revisión de incidentes por parte del personal de soporte, los administradores de bases y el personal de operaciones ha disminuido ya que al existir menos incidentes realizan menos revisiones y pruebas diarias.

La disminución de los incidentes ha hecho que la administración realice cambios a nivel del número de personas que están en el área de soporte, ya que las estadísticas indican que existe una disminución del 30% de incidentes reportados por lo cual 2 personas de soporte I y una de soporte II están siendo cambiadas a desarrollo para mejorar los

tiempos de entrega en los nuevos requerimientos que la dirección solicita.

Tabla 81 Tabla de Incidentes 2016

Mes	Cantidad
Enero	123
Febrero	106
Marzo	115
Abril	100
Mayo	135
Junio	111
Julio	117
Agosto	104
Septiembre	121
Octubre	80
Noviembre	68
Diciembre	64

En la tabla se explica la cantidad de incidentes mensuales, y la disminución de los mismos a partir de las políticas implementadas.

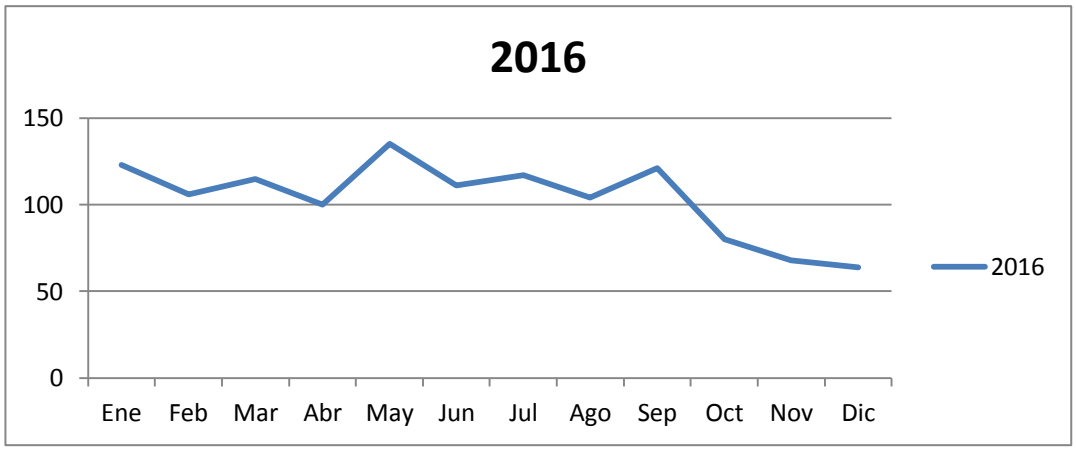


Figura 6.1 Tendencia de los Incidentes de 2016

También se han mejorado las relaciones laborales entre departamentos lo que se ve reflejado en la productividad según las estadísticas de la administración los departamentos han incrementado la productividad en un 8% esto debido a que ya no se pierde tiempo en reuniones para definir quienes resolverán los incidentes reportados lo que conlleva realizar nuevas pruebas y actualizaciones con los usuarios.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1 La información es el activo más importante para la vida de las personas y de las empresas, es por ello que es sustancial que este activo este seguro, disponible y que sea confiable cuando se lo requiera, además es fundamental acoger las recomendaciones que dan las normas ISO en especial la 27002/IEC.

2 Mediante una encuesta al personal de las diferentes áreas del DS se pudo determinar el nivel de conocimiento de seguridad informática con el cual se cuenta en la actualidad, el resultado ayudo a determinar qué puntos de la norma debían ser atendidos.

3 Se ha realizado un informe con el detalle de los escenarios y las consecuencias que se podrían dar si se materializa el riesgo, para que la información sea de completa ayuda para la organización la misma cuenta con el estado inicial del riesgo y el estado ya como riesgo residual lo que permite evaluar el impacto obtenido con la aplicación de las políticas.

4 Se ha diseñado una Política de Seguridad de la Información, con tres de los dominios de la Norma ISO 27002 /IEC, para mitigar los riesgos que se puedan presentar en la seguridad de la información de la organización, se determinó la situación actual con la cual se pudo describir un proceso específico con el que se desarrolló

5 El cumplimiento de las políticas de seguridad no garantiza la eliminación del riesgo, pero su cumplimiento si garantiza la mitigación del mismo, esto debido a que el riesgo siempre estará presente pero con la ayuda de las políticas este disminuirá considerablemente que ese riesgo se materialice.

6 La metodología OCATAVE ALLEGRO para el análisis de riesgos, permitirá de forma sencilla y oportuna a través de sus plantillas identificar la probabilidad y el impacto de los riesgos y así poder establecer los controles para su mitigación o prevención.

7 Luego del análisis y el diseño la política fue implementada tomando los controles recomendados por el estándar ISO/IEC 27002:2013 y por último se realizó la difusión con el objetivo de que el personal del departamento y la empresa tomen conciencia de las políticas y adquieran una cultura de seguridad. Dentro de la difusión se enfoca los objetivos de la política y como nos ayudan a realizar de forma segura nuestras actividades.

RECOMENDACIONES

1 Realizar un análisis periódico con el fin de detectar las amenazas que día a día van surgiendo y pueden suponer un riesgo a la seguridad de la información.

2 Se recomienda tener una persona y/ o un departamento encargado del control y monitoreo de forma constante de las políticas así como de las actualizaciones que se presenten dentro de la norma y metodología aplicada.

3 Se debe trabajar constantemente en la concientización al personal de la organización ya que esto es fundamental para que la política tenga éxito y la misma puede mantenerse vigente en el tiempo.

4 Se recomienda continuar el desarrollo e implementación de los demás controles de la norma para con ello llegar a tener un SGSI y luego de ello el siguiente paso adaptarlo a una norma certificable.

5 Especializar y certificar a personas de la empresa con el fin de realizar auditorías internas y realizar evaluaciones sobre la política, con esto se evitaran los altos costos de la contratación de consultores externos.

BIBLIOGRAFÍA

[1] Wikipedia, Círculo de Deming, https://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming , fecha de consulta Octubre de 2016.

[2] Portal ISO 27001 España, Norma ISO27001. http://www.iso27000.es/iso27000.html, Octubre de 2016.

[3] CERT, OCTAVE Allegro Method, http://www.cert.org/resilience/products-services/octave/octave-allegro-download.cfm , Noviembre de 2016.

[4] ENS, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html, Octubre de 2016.

[5] Fernando Moreno, Norma Técnica Colombiana NTC-ISO 27005, http://es.slideshare.net/danger-leinad/iso-27005espanol, Noviembre de 2016.

[6] Wikipedia, ISO/IEC 27002, https://es.wikipedia.org/wiki/ISO/IEC_27002, Noviembre de 2016

[7] Agustín López, Controles ISO 27002, http://www.iso27000.es/download/ControlesISO27002-2013.pdf , Noviembre de 2016.

[8] ISO, ISO/IEC 27002:2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533 , Octubre de 2016

[9] Organización Internacional para la Estandarización (ISO). http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm , Octubre de 2016.

[10] LACCEI, Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002, http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf , Diciembre de 2016.

[11] Ramón Robles, Álvaro Rodríguez de Roa, La gestión de la seguridad en la empresa: La gestión de la en la empresa, https://www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128 , Noviembre de 2016.

[12] Manuel Collazos La nueva versión ISO, http://www.cip.org.pe/index.php/eventos/conferencias-ceremonias-y-patrocinios/item/download/125_2f7be404f0dba27dabc8efd91bd14668.html, Noviembre de 2016

[13] Agustín López Neira, Controles ISO 27002,

http://www-2.dc.uba.ar/materias/seginf/material/Clase_22-ISO17799_vf.pdf , fecha de consulta Noviembre de 2016.

[14] UBA, Código de práctica para la gestión de la seguridad de la información, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533 , Diciembre de 2016

[15] Blanca Duque, Metodologías de Gestión de Riesgo, https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf , Diciembre de 2016.

ANEXOS

Anexo A Encuesta realizada

1. ¿Tiene conocimiento de sus responsabilidades referente a la seguridad de la información?
   Sí __ No__

2. ¿Ha firmado usted un acuerdo de confidencialidad de la información?
   Sí__ No__

3. ¿Su área cuenta con controles de acceso de personal?
   Sí__ No__

4. ¿Los equipos y Sistemas que utiliza cuentan con contraseña única para Usted?
   Sí __ No__

5. ¿Se realiza mantenimiento periódico de hardware y software?
   Sí __ No__

6. ¿El área cuenta con controles como, antivirus antispyware?
   Sí __ No__

7. ¿Se realizan Copias de Seguridad de la Información?
   Sí __ No__

8. ¿En qué medio se almacenan los respaldos?_____

9. ¿Con que periodicidad se realizan? _____

10. ¿Cuentan con programas para la encriptación de datos?
    Sí __ No__

11. ¿Cuenta su departamento con control de cambios para los desarrollos?
    Sí __ No__

12. ¿Al presentarse un incidente de seguridad, se cuenta con un plan de contingencia?
    Sí __ No__

13. ¿Se tiene una matriz de pruebas para los pasos de desarrollo a producción?
    Sí __ No__

14. ¿Se mantiene una bitácora de los equipos que se dan de baja en su área?
    Sí __ No__

15. ¿Tiene un acceso único para conexión con las Bases de Datos?
    Sí __ No__

16. ¿Cuenta con ambiente de desarrollo y pre-producción?
    Sí __ No__

17. ¿Los usuarios del personal que han salido de la empresa se encuentran inactivos?
    Sí __ No__

Anexo B Documentos indicados en la política

SOLICITUD DE ACCESO AL SISTEMA	
NOMBRE DEL SOLICITANTE	
DEPARTAMENTO	
CARGO	
NOMBRE DEL SISTEMA	
PERMISOS DE:	
CONSULTA	
INGRESO	
MODIFICACION	
MODULO	
FECHA DE LA SOLICITUD	
FIRMA DEL SOLICITANTE	
FIRMA JEFE DEL AREA	
FIRMA DIRECCION DE SISTEMAS	

Adicional revalidaran todos los accesos de los usuarios para asegurarse que solo los usuarios designados tengan permisos de administrador.

SOLICITUD DE MODIFICACION DE FUENTES	
NOMBRE DEL SOLICITANTE	
DEPARTAMENTO	
CARGO	
NOMBRE DEL FUENTE	
DESCRIPCION DEL CAMBIO	
MODULO	
FECHA DE LA SOLICITUD	
FIRMA DEL SOLICITANTE	
FIRMA JEFE DEL AREA	
FIRMA DIRECCION DE SISTEMAS	

CATÁLOGO DE TAREAS DE PRUEBAS FUNCIONALES
ESPECIFICACIÓN DE LAS PRUEBAS
Descripción: Acceso del usuario a la aplicación. **Código**: Secuencia Numérica Única **Objetivo:** Comprobar que sólo los usuarios autorizados tienen acceso a la aplicación.
Prueba a realizar: Comprobar que un usuario autorizado tiene acceso a la aplicación. **Prueba a realizar:** Comprobar que un usuario autorizado con una clave incorrecta no puede acceder. **Prueba a realizar:** Comprobar que un usuario no autorizado recibe un mensaje apropiado sobre la negación del acceso solicitado **Prueba a realizar:** Comprobar que no pueda acceder un usuario no registrado en el sistema.

CATÁLOGO DE TAREAS DE PRUEBAS FUNCIONALES
ESPECIFICACIÓN DE LAS PRUEBAS
Descripción: Consulta de Aplicación. **Código**: Secuencia Numérica Única **Objetivo:** Comprobar que la aplicación devuelve la información correcta que el usuario solicita. **Precondiciones:** El usuario debe tener acceso a la aplicación.
Prueba a realizar: Con un usuario autorizado ingresar al sistema y verificar la información que entrega. **Prueba a realizar:** Comprobar que la información que se entrega está completa.
CATÁLOGO DE TAREAS DE PRUEBAS FUNCIONALES
ESPECIFICACIÓN DE LAS PRUEBAS
Descripción: Prueba con Usuario Final. **Código**: Secuencia Numérica Única **Objetivo:** Comprobar que el usuario seleccionado puede realizar la prueba en su estación de trabajo
Prueba a realizar: Comprobar que el usuario autorizado tiene acceso a la aplicación. **Prueba a realizar:** Con el usuario autorizado ingresar al sistema y verificar la información que entrega. **Prueba a realizar:** Comprobar que el usuario autorizado recibe la información completa solicitada

CATÁLOGO DE TAREAS DE PRUEBAS FUNCIONALES
CONTROL DE CAMBIOS
Descripción: Indicar las modificaciones realizadas a la Aplicación. **Código**: Secuencia Numérica Única **Objetivo**: Llevar un control de los cambios realizados a los aplicativos
Fecha: Indicar fecha del cambio
Desarrollado: Usuario que desarrolla el cambio
Solicitado Departamento / Persona que realiza el cambio
Cambios Realizados: Especificar las modificaciones realizadas
Codificación: Agregar códigos de las tablas en las que se hicieron las solicitudes así como los códigos pruebas de desarrollo y Usuario