ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"TRATAMIENTO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN PARA EL PROCESO DE DESARROLLO DE SISTEMAS DE EMPRESA DE SOLUCIONES INFORMÁTICAS"

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DE TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

LUIS MANUEL MORA TORRES

GUAYAQUIL - ECUADOR

2018

AGRADECIMIENTO

Agradezco a Dios por darme las fuerzas para terminar este trabajo y poder cumplir con una meta más en mi vida profesional. Le doy gracias a mis padres, Luis y Glenda, y a mi hermano Carlos, quienes no dejaron que me rindiera cuando mi fuerza de voluntad para dedicar el esfuerzo requerido decaía. Agradezco también a mi amor, Tatiana, quien con su comprensión y paciencia me ayudó a mantenerme dedicado al proyecto. Finalmente agradezco a mis amigos, quienes con sus consejos permitieron despejar dudas y así poder cumplir con el objetivo trazado.

DEDICATORIA

Dedico este trabajo a mis padres quienes con su esfuerzo y sacrificios lograron darme una educación de calidad, me han apoyado y lo seguirán haciendo en cada nueva etapa de mi vida. También dedico este trabajo a mi compañera de vida, Tatiana, a mi familia y a mis amigos que han estado en los buenos y malos momentos de mi vida.

TRIBUNAL DE SUSTENTACIÓN

_____

PH. D. CRISTINA ABAD ROBALINO

PRESIDENTE DEL TRIBUNAL

_____

MGS. LENIN FREIRE COBO

DIRECTOR DEL TRABAJO DE TITULACIÓN

_____

MGS. RONNY SANTANA ESTRELLA

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

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

_____

ING. LUIS MORA TORRES

RESUMEN

Por lo general, cuando se refiere a la seguridad en el desarrollo de software, existe la tendencia de analizar los riesgos y aplicar controles de seguridad al sistema en desarrollo, sin embargo, el proceso desde la toma de requerimientos hasta la puesta en producción puede aparecer riesgos en ese proceso, por lo que es necesario que realice una gestión de riesgos independiente. El presente trabajo de titulación desarrollado a lo largo de cinco capítulos tiene como objetivo el tratamiento de riesgos para el proceso de desarrollo de sistemas.

En el proceso de realizar el tratamiento de riesgos, se comienza con la identificación de los activos, que conforman el proceso de desarrollo de software, luego se realiza un análisis de riesgos en función de las amenazas, vulnerabilidades y principios de seguridad, luego se determina el nivel de riesgos que se va a tratar y que deben ser atendidos de manera inmediata para poder aplicar un tratamiento adecuado a través de actividades planificadas. Finalmente se plantea unos casos con amenazas al proceso y se explica cómo funcionarían los controles de seguridad aplicados en la norma ISO/IEC 27001:2013.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

ERP : Enterprise Resource Planning

IEC : International Electrotechnical Commission

ISO : International Organization for Standardization

SGSI : Sistema de Gestión de Seguridad de la Información

TIC : Tecnologías de Información y de la Comunicación

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

El proceso de desarrollo de software evoluciona constantemente debido a la aparición de nuevas herramientas, metodologías debido a nuevas soluciones y desafíos producido por el aumento en el uso de la tecnología

en las empresas. Algunas de estas empresas de desarrollo de sistemas usan servicios de control de código fuente, trabajadores remotos, almacenamiento en línea y servidores virtuales en la nube lo que les ha permitido aumentar considerablemente la velocidad de creación y puesta en producción de nuevos sistemas, sin embargo, el uso de estas nuevas herramientas aumenta los riesgos de estos sistemas de información debido a nuevas amenazas que aparecen debido a la exposición de nuevos actores lógicos y humanos.

Las tendencias en seguridad de información actuales abarcan cada vez más aspectos de la vida cotidiana. En el año 2017 tuvo entre sus principales amenazas el secuestro de información, debido a la aparición de ramsonware, ataques a infraestructuras críticas, seguramente por la recopilación de información personal no autorizada y la venta de esta información sin conocimiento de los usuarios [1]. La materialización de estas amenazas ha causado impacto negativo en las empresas, en su imagen, en sus clientes, resultando el aumento del interés en crear esquemas de seguridad.

Cuando un cliente contrata una empresa para el desarrollo de un sistema, no solo deposita su confianza en la funcionalidad del sistema, sino que espera también una adecuada gestión de seguridad de la información. También espera que los productos y servicios contratados tengan sus

propios esquemas de seguridad para que no afecte su funcionalidad, proteja su información, genere pistas de auditoría que permita disminuir los riesgos en su negocio. Por esto, es de suma importancia que se tenga claro que en el desarrollo de un sistema no solo la empresa proveedora tiene riesgos que tratar, sino que no debe de transmitir riesgos que puedan causar un daño a su cliente.

1.2 DESCRIPCIÓN DEL PROBLEMA

La empresa desarrolladora de software fue creada a partir de la necesidad de un grupo de empresas de compra y venta de productos agrícolas que necesitaban una solución que permita gestionar sus procesos de manera centralizada y no se encontró en el mercado una solución que satisfaga sus necesidades. El producto estrella de la empresa desarrolladora de software es un ERP implementado en la nube, el cual está en constante evolución, pero de forma controlada.

Debido a que es un ERP especializado, los clientes comparten mucha información confidencial de sus negocios y se ha vuelto necesario asegurar la seguridad de la información en los procesos internos de la empresa de tal manera que los clientes se sientan tranquilos y confiados.

La empresa, en sus inicios solo se enfocaban en el proceso de desarrollo de software, pero han visto la necesidad de proteger este proceso con un

esquema de seguridad en el proceso y en el producto, como valor agregado a sus clientes.

1.3 SOLUCIÓN PROPUESTA

La propuesta consiste en hacer una identificación de los activos de información relevantes al proceso de desarrollo de software, hacer una identificación de los riesgos de seguridad de información, evaluar el impacto en caso de materializarse estos riesgos y a partir de esto generar una política de seguridad de información basándose en los controles de la norma ISO/IEC 27002:2013.

1.4 OBJETIVO GENERAL

Realizar el tratamiento de riesgos de seguridad de información para el proceso de desarrollo de sistemas del departamento de empresa de soluciones informáticas.

1.5 OBJETIVOS ESPECÍFICOS

- Identificar los activos de información y los riesgos de seguridad de información en el proceso de desarrollo de software.
- Evaluar la probabilidad y el impacto en caso de materializarse los riesgos de seguridad de información.
- Desarrollar un plan de tratamiento de los riesgos identificados.

1.6 METODOLOGÍA

La gestión de riesgos consiste en identificar y analizar los riesgos para posteriormente hacer un tratamiento adecuado.

En primer lugar, se realizará una revisión del estado actual de la empresa y cuáles son los roles y funciones en el proceso de desarrollo de sistemas.

Para poder hacer el análisis de riesgos es necesario identificar los activos de información de la empresa valiosos en el proceso de desarrollo de sistemas. Cada uno de estos activos deben ser valorados en función de su importancia en cuanto a la seguridad de información.

Lo siguiente que se hará es identificar las amenazas. Cada activo tiene amenazas que en caso de materializarse pueden producir un incidente de seguridad en la empresa.

Una vez valorados los activos e identificadas sus amenazas se procederá a determinar la probabilidad de ocurrencia de los incidentes de seguridad y el impacto en el proceso, es decir, se identificarán los riesgos y esto permitirá tomar decisiones respecto la manera más apropiada de tratarlos.

La evaluación de riesgos permite saber si se deberá mejorar los controles de seguridad existentes o si se deben aplicar nuevos controles. Ciertos riesgos se los podrá asumir, pero otros por el costo deberán tratar de ser transferidos o evitados. Esto dependerá de la relación costo/beneficio para

la empresa con lo cual se procede a la creación de un plan de tratamiento de riesgos.

Finalmente se debe establecer un procedimiento para el seguimiento de los proyectos dentro del plan de tratamiento de riesgos.

Figura 1.1 Procesos de la Gestión de Riesgos

Fuente: Autor

Existen algunas metodologías para gestionar riesgos sin embargo en este trabajo se ha escogido MAGERIT versión 3 debido a que es de carácter público, y cuenta con una guía paso a paso de cómo realizar el análisis de riesgos además de un catálogo de elementos que aparecen en un proyecto de gestión de riesgos.

CAPÍTULO 2

MARCO TEÓRICO

2.1 SEGURIDAD DE LA INFORMACIÓN

Históricamente se tiende a confundir la seguridad informática con la seguridad de información debido a que se califica esta última como algo

técnico y complicado. Sin embargo, no son lo mismo y no es necesario que un profesional de la seguridad de información tenga profundos conocimientos técnicos.

La seguridad informática “es la forma como se detallan las implementaciones técnicas de la protección de la información, el despliegue de antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo”. En cambio, la seguridad de información “es la disciplina en el arte y ciencia de la protección, de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información” [2].

Los pilares sobre los que se basa la seguridad de información son la confidencialidad, disponibilidad e integridad [3].

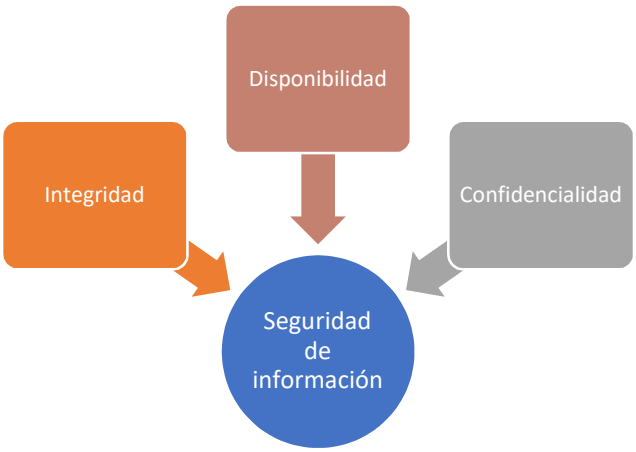

Figura 2.1 Pilares de la seguridad de información.

Fuente: Autor

La confidencialidad se refiere a proteger la información de acceso no autorizado, es decir, una falla en mantenerla significa que alguien tuvo acceso a información sensible que no debía conocer. Una falla en la confidencialidad en un negocio puede tener consecuencias graves como revelación de estrategias comerciales o pérdida de reputación en los casos en los que se aloja datos de clientes.

La disponibilidad implica que la información puede ser accedida por quien esté autorizado cuando la necesite.

La integridad involucra mantener la información sin alteración por parte de terceros no autorizados, además no debe cambiar en su transporte o

mientras esta almacenada. La información debe ser confiable para quien la necesite.

Para poder cumplir con la protección de la información en una empresa, es necesaria una adecuada gestión de riesgos. La gestión de riesgos incluye el análisis de los riesgos que pueden existir, el evaluar su impacto en diversos ámbitos y hacer un tratamiento adecuado para mitigar sus efectos.

2.2 CONCEPTOS EN ANÁLISIS Y EVALUACIÓN DE RIESGOS

Para poder entender lo que abarca el análisis y evaluación de riesgos es importante conocer las siguientes definiciones [4]:

Activo: Es aquello que tiene algún valor para su propietario, es susceptible de ser atacado y su no disponibilidad o deterioro supone graves consecuencias por lo que debe ser protegido. Puede ser tangible o intangible.

Amenaza: Causa potencial de un incidente no deseado que puede causar perjuicio a las operaciones de la empresa (misión, funciones, imagen o reputación), a los activos de información (acceso no autorizado, destrucción, modificación o revelación no autorizada de información), a los individuos que trabajan para la organización o a los asociados (proveedores, clientes).

Vulnerabilidad: Es la ausencia o ineficacia de los controles de seguridad que protegen el valor de un activo de información. Es decir, es una debilidad en un sistema de información o un procedimiento de seguridad.

Probabilidad: Posibilidad de que ocurra un evento.

Impacto: Es el costo de un incidente para la empresa. Es el resultado de un evento.

Riesgo: Es la probabilidad de que una amenaza explote alguna vulnerabilidad teniendo impacto sobre los activos y provocando consecuencias negativas a la empresa.

Para la identificación de los riesgos más importantes primero hay que identificar los activos, vulnerabilidades y sus respectivas amenazas.

La evaluación de riesgos incluye determinar el grado al cual eventos adversos pueden impactar a la empresa. Se debe tomar factores como la misión de la empresa, las regulaciones vigentes en el país donde opera, al nivel de riesgo tolerado por la Administración y el presupuesto. Existen otros factores a tomar en cuenta como las condiciones económicas del país, las tendencias del mercado, surgimiento de nueva competencia o posibilidad de ocurrencia de desastres naturales.

Una vez identificado un riesgo y teniendo en cuenta su impacto, entonces existen cuatro alternativas para tratarlo que son [5]:

- Evitar el riesgo, esto implica cambiar o dejar de hacer ciertas actividades o procesos que causan los riesgos. Por ejemplo, un incidente como lo puede ser la pérdida de un equipo con información sensible se puede evitar prohibiendo que se lo saque de las oficinas.
- Mitigar el riesgo, es decir, se aplican estrategias para reducir la probabilidad de ocurrencia o el impacto si se materializa.
- Trasladar el riesgo. Se transfiere el impacto a un tercero, pero no elimina el riesgo. Por ejemplo, se contrata una empresa de seguros.
- Aceptar el riesgo, es decir, la administración de la empresa conoce el riesgo y puede establecer una política a seguir en caso de materializarse o simplemente no hacer nada al respecto.

2.3 NORMA ISO/IEC 27002:2013.

La familia de normas ISO/IEC 27000 son un conjunto de estándares que contienen mejores prácticas para la gestión de la seguridad de la información. Son creadas y publicadas por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). estándares de esta familia son aplicables a organizaciones de cualquier tamaño y sector.

La norma principal es la ISO/IEC 27001:2013 que se enfoca en definir los requisitos para el Sistema de Gestión de Seguridad de Información (SGSI) de una organización. Un SGSI consiste en procedimientos y medidas que

normalizan la gestión de la seguridad de la información, ya sea de toda una empresa o de uno de sus procesos de negocio. Esta norma puede ser auditada y certificada. El resto de las normas de la familia ISO/IEC 27000 son guías de buenas prácticas que ayudan a la implementación de la norma principal [6].

La ISO/IEC 27002:2013 es un manual de buenas prácticas que permiten a una empresa mejorar la seguridad de información. En su versión del año 2013 se estructura en 14 dominios (secciones de seguridad), 35 objetivos de control (aquello que se quiere conseguir), 114 controles que se pueden implementar. No todos los controles son aplicables a cada organización [7].

2.4 METODOLOGÍA MAGERIT VERSIÓN 3.

MAGERIT es una metodología que permite al análisis y la gestión de riesgos que son consecuencia del desarrollo y uso de sistemas de información. Ha sido elaborada por el Consejo Superior de Administración Electrónica de España para minimizar los riesgos de la implantación y uso de las tecnologías de la información y está disponible para cualquier organización pública o privada que desee ponerla en práctica [8].

Los objetivos de MAGERIT versión 3 son concientizar acerca de la existencia de los riesgos del uso de las tecnologías de información y comunicaciones (TIC) y la necesidad de gestionarlos; propone un método

para analizar los riesgos y ayuda a planificar el tratamiento de estos para mantenerlos en un nivel aceptable para la empresa que la aplica.

La versión 3 de esta metodología fue elaborada en el año 2012 y se encuentra compuesta por dos libros y una guía de técnicas.

Libro 1: Método. En este libro se presentan las actividades de análisis y tratamiento de riesgos. Las actividades mencionadas son la Caracterización de activos, Caracterización de amenazas, Caracterización de salvaguardas y estimación del estado de riesgo.

Libro 2: Catálogo de Elementos. Este libro propone elementos estándar los cuales pueden ser utilizados con el objetivo de centrarse en la tarea del análisis y en lo estandarizar sus resultados. Estos elementos se agrupan en tipos de activos, dimensiones de valoración de los activos, criterios de valoración de activos, amenazas típicas y salvaguardas.

Guía de técnicas. Este libro incluye algunas técnicas específicas y generales que se pueden emplear para llevar a cabo los proyectos de análisis y gestión de riesgos.

CAPÍTULO 3

ANÁLISIS Y DISEÑO DEL TRATAMIENTO DE RIESGOS

3.1 SITUACIÓN ACTUAL

La empresa de desarrollo de sistemas fue fundada en Junio del año 2014. Es una empresa ecuatoriana con inversión extranjera que fue creada con el objetivo de brindar servicios de consultoría y desarrollo de sistemas para un grupo multinacional de compra y venta de productos agrícolas las cuales durante muchos años realizaron sus operaciones utilizando

programas de ofimática en el día a día. Se identificó la oportunidad de brindar soluciones personalizadas que les permitiera gestionar su información principalmente en las áreas Comercial y Logística. Actualmente existen proyectos para ampliar las soluciones a las áreas de Producción y Financiera.

El producto principal de la empresa es un Sistema de Planificación de Recursos Empresariales (ERP por sus siglas en inglés) el cual incluye los siguientes módulos:

- Administración. Permite el ingreso de diversos catálogos al sistema.
- Contratos. Este módulo tiene la información de los contratos agrícolas y registra información de contrapartes en las transacciones comerciales, precios de los productos y otras condiciones generales de la negociación.
- Logística. Contiene información de cantidades a despachar, lugar de destino, fechas estimadas de envío y entrega, etc.
- Inventario. Mantiene la información de los productos y sus movimientos entre bodegas.

Adicional a los servicios de implementación y soporte derivados de su producto estrella, la empresa también ofrece servicios de consultoría para la automatización de procesos y desarrollos de software específicos no relacionados al ERP.

La empresa no tiene oficinas propias, alquila una oficina para los desarrolladores en edificio sin guardianía privada. Cuenta con colaboradores dentro y fuera del país siendo una de sus características el permitir el trabajo remoto, por lo que la comunicación vía Skype es la principal manera de compartir ideas.

En cuanto a infraestructura informática, la empresa posee servidor propio para almacenamiento de datos, sin embargo, para probar todas las aplicaciones y herramientas se utilizan servidores virtuales en la nube de Microsoft Azure.

Algunas de las actividades de seguridad implementadas son:

- Inclusión de cláusula de confidencialidad en contrato con los empleados.
- Instalación de antivirus en las laptops de desarrolladores y
- Uso de firewall en la red de la oficina.

3.2 PROCESO DE DESARROLLO DE SISTEMAS

La función principal es diseñar y programar las tareas asignadas basadas en los requerimientos de los clientes.

Este proceso consta de 4 fases tal como se puede apreciar en la siguiente figura:

Figura 2.1 Fases en el proceso de desarrollo de sistemas.

Fuente: Autor

El proceso termina cuando se implementa el sistema para revisión de cliente. En el caso que el cliente requiera un cambio, vuelve a iniciar el proceso descrito anteriormente.

La empresa cuenta actualmente con un grupo de profesionales con diferentes roles relacionados a la tecnología, entre los que podemos encontrar:

- Desarrolladores de Software. Personal especializado en desarrollar aplicaciones web o móviles. Se especializan en tecnologías Microsoft.

- Líderes de Desarrollo. Son desarrolladores que adicionalmente tienen la tarea de revisar que las tareas asignadas a sus compañeros cumplan con los requerimientos solicitados por el Jefe de Proyectos.
- Jefe de Desarrollo. Encargado de la coordinación de todo lo relacionado a desarrollo de software, es decir, elaborar los planes de trabajo, proponer buenas prácticas de desarrollo, etc.
- Gerente de Proyectos. Encargado de reunirse con los usuarios, jefes departamentales y gerentes en las empresas para identificar los requerimientos y en conjunto con el Jefe de Desarrollo plantear soluciones.

Dentro de este grupo de profesionales, no se cuenta con un especialista que gestione la seguridad al interior de la empresa.

3.3 INVENTARIO DE ACTIVOS DE INFORMACIÓN

Es esta sección se procederá con la Identificación de activos de información asociados al proceso de desarrollo de sistemas de la empresa.

Para clasificarlos se han usado los tipos de activo propuestos en el libro de catálogo de elementos de MAGERIT versión 3.

Tabla 1. Activos de información de la empresa

Tipo	Código	Nombre	Descripción
Datos Información	DI001	Documentación	Especificación y documentación de los nuevos desarrollos
Datos Información	DI002	Código fuente	Código fuente de las aplicaciones ofrecidas
Datos Información	DI003	Manuales	Manuales de uso del sistema
Datos Información	DI004	Datos de prueba	Datos de prueba lo más cercano a la realidad
Datos Información	DI005	Datos de configuración	Datos de configuración de las aplicaciones
Software	SO001	Ofimática	Programas para gestionar documentación
Software	SO002	Visual Studio	Software para Desarrollo
Software	SO003	Motor Base Datos	Sistema de Gestión de Base de Datos
Software	SO004	Team Foundation Server	Sistema de Control de versiones
Software	SO005	Antivirus	Antivirus instalado en máquina de desarrolladores

Tipo	Código	Nombre	Descripción
Software	SO006	Internet Information Services	Permite alojar aplicaciones web
Hardware	HA001	Laptops	Laptops usadas por el personal
Hardware	HA002	Servidor interno	Servidor de archivos y de pruebas local
Hardware	HA003	Servidor virtual Pruebas	Servidor en Microsoft Azure para uso durante proceso de desarrollo o durante presentaciones a clientes.
Hardware	HA004	Router	Equipo que permite conectar la red de oficina con internet
Hardware	HA005	Firewall	Equipo que protege la red de la oficina de intrusiones externas.
Soporte de Información	SI001	Disco externo	Disco externo con instaladores y respaldos
Redes de comunicaciones	CO001	Internet	Acceso a Internet
Redes de comunicaciones	CO002	Red local	Red local en la que se encuentran los dispositivos de la empresa
Instalaciones	IN001	Oficina	Oficina donde se desarrollan las actividades de la empresa
Personal	PE001	Desarrollador	Desarrollador

Tipo	Código	Nombre	Descripción
Personal	PE002	Jefe de Desarrollo	Jefe de Proyecto
Personal	PE003	Usuario de prueba	Usuario

Dependencia entre Activos

Los activos pueden estar relacionados de tal manera que, si una amenaza afecta un activo de nivel inferior, este puede llegar a afectar a un activo de nivel superior. El análisis de la dependencia de activos poder hacer una mejor valoración de los riesgos.

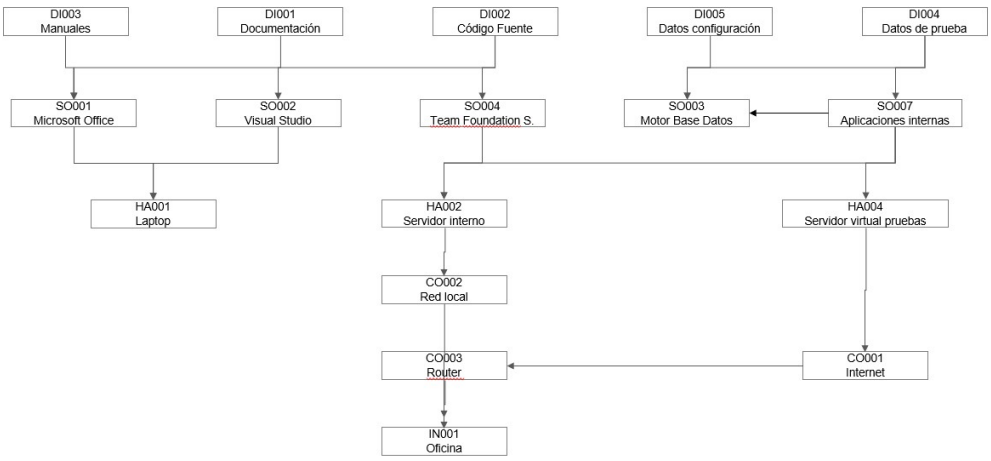

Figura 3.2 Diagrama de dependencia de activos

Fuente: Autor

La seguridad de los activos de información de nivel superior como el código fuente o la documentación de los proyectos al estar en formato digital dependen principalmente del sistema operativo. Hay activos como el servidor virtual el cual sin conexión a Internet no se puede acceder.

3.4 VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Una vez realizadas las tareas de identificación de activos y dependencia entre activos toca analizar cuál es el valor de cada uno de ellos para la empresa en el proceso de desarrollo.

Esta valoración que se asigna a cada activo depende de un criterio subjetivo de las personas involucradas en el proceso quienes determinarán que tan valioso es cada activo y por lo tanto que tan necesaria es su protección.

Cada activo es valorado en una o más dimensiones de seguridad dependiendo de si es relevante o no. Las dimensiones de seguridad son características que hacen valioso un activo. En el caso del proceso de desarrollo de sistemas, se valorará la confidencialidad, la disponibilidad y la integridad de los datos.

El resultado de la tarea de valorar activos se conoce en MAGERIT versión 3 como modelo de valor el cual no es más que un reporte que indica el valor asignado en cada una de las dimensiones de seguridad. Para valorar los activos se hizo uso de las siguientes escalas de valores:

Tabla 2. Escala de valoración de confidencialidad

Valor	Descripción
1	Información disponible para todo personal interno o externo.
2	Información restringida que si es conocida podría causar efectos indeseados. Limitada al personal de la empresa.
3	Información confidencial que si es conocida podría dañar o perjudicar el proceso de desarrollo.
4	Información reservada que si es conocida implicaría daños serios al proceso de desarrollo.
5	Información secreta que si es conocida implicaría un daño excepcionalmente grave al proceso de desarrollo.

Tabla 3. Escala de valoración de integridad

Valor	Descripción
1	No aplica o alteración no afecta ninguna tarea del proceso
2	Modificación o destrucción no autorizada afectaría levemente una o varias tareas del proceso.
3	Modificación o destrucción no autorizada afectaría alguna de las tareas, pero el proceso en su conjunto no es afectado.

4	Modificación o destrucción no autorizada afectaría de manera grave el proceso.
5	Modificación o destrucción no autorizada impediría afectaría de manera extremadamente grave al proceso.

Tabla 4. Escala de valoración de disponibilidad

Valor	Descripción
1	Afectación menor sobre una tarea específica o ninguna afectación sobre las actividades del proceso.
2	Afectación en el cumplimiento de alguna de las actividades del proceso.
3	Perjuicio en el cumplimiento eficaz de las actividades del proceso.
4	Daño grave que interrumpiría las actividades del proceso
5	Daño excepcionalmente grave que interrumpiría las actividades del proceso de desarrollo y de otros procesos de la empresa.

Tabla 5. Importancia de activos de acuerdo a su valoración

Valor	Importancia	Notación	Descripción
1	Muy Baja	MB	No aplica el criterio para el activo
2	Baja	B	Daño menor, no se afecta el proceso.

3	Media	M	Daño importante, se afecta de forma parcial al proceso.
4	Alta	A	Daño grave. Uno o varios procesos son afectados.
5	Muy Alta	MA	Daño muy grave. Se pone en juego la credibilidad de la empresa.

En la Tabla 6, se presenta el modelo de valor de los activos del proceso de desarrollo. Luego de hacer una valoración en las dimensiones de confidencialidad, integridad y disponibilidad se calcula un promedio y de acuerdo a la escala de la Tabla 5 se le asigna a cada activo un nivel de importancia.

Tabla 6. Modelo de valor de los activos

Código	Descripción	C	I	D	Valor	Criticidad
DI001	Documentación	4	4	3	4	A
DI002	Código fuente	5	5	5	5	MA
DI003	Manuales	2	3	3	3	M
DI004	Datos de prueba	2	3	3	3	M
DI005	Datos de configuración	3	3	3	3	M
SO001	Ofimática	1	2	3	2	B
SO002	Visual Studio	2	4	5	4	A
SO003	Motor Base Datos	2	4	5	4	A
SO004	Team Foundation Server	2	4	5	4	A
SO005	Antivirus	1	1	2	1	MB
SO006	Internet Information Services	1	3	3	2	B
SO007	Aplicaciones internas	4	3	3	3	M

HA001	Laptops	4	3	5	4	A
HA002	Servidor interno	4	3	4	4	A
HA003	Servidor virtual Pruebas	4	3	4	4	A
HA004	Router	1	4	5	3	M
HA005	Firewall	3	3	3	3	M
SI001	Disco externo	4	3	3	3	M
CO001	Internet	1	2	5	3	M
CO002	Red local	3	2	5	3	M
IN001	Oficina	1	3	4	3	M
PE001	Desarrollador	3	1	5	3	M
PE002	Jefe de Proyecto	4	1	5	3	M
PE003	Usuario de prueba	1	1	2	1	MB

3.5 ANÁLISIS DE AMENAZAS Y VULNERABILIDADES

Una vez levantado el modelo de valor con los activos más importantes, el objetivo es elaborar el mapa de riesgos del proceso identificando las amenazas y dándoles un valor de afectación sobre los activos de información.

Las amenazas se aprovechan de las vulnerabilidades, es decir, de las debilidades en los activos o en los controles de seguridad que tienen implementados. En la tabla 7 se ha identificado amenazas haciendo uso del libro de catálogo de elementos de MAGERIT versión 3 junto con una vulnerabilidad asociada.

Tabla 7. Amenazas y vulnerabilidades asociadas a los activos

Tipo de Activo	Activo	Amenaza	Vulnerabilidad
Datos / Información	Documentación	Alteración accidental de la información	Cualquier usuario puede acceder y modificar los archivos en el servidor
Datos / Información	Documentación	Modificación deliberada de información	Cualquier usuario puede acceder y modificar los archivos en el servidor
Datos / Información	Documentación	Destrucción de la información	Cualquier usuario puede acceder y modificar los archivos en el servidor
Datos / Información	Documentación	Divulgación de información	Uso sin restricción de medios extraíbles e internet
Datos / Información	Código fuente	Alteración accidental de la información	Código fuente puede ser modificado en cualquier momento por cualquier desarrollador
Datos / Información	Código fuente	Destrucción de la información	Código fuente puede ser modificado en cualquier momento por cualquier desarrollador
Datos / Información	Código fuente	Divulgación de información	Código fuente puede ser copiado. Uso sin restricción de medios extraíbles e internet.
Datos / Información	Manuales	Destrucción de la información	Manuales pueden ser borrados en cualquier momento
Datos / Información	Manuales	Divulgación de información	Manuales pueden ser copiados en cualquier momento
Datos / Información	Datos de prueba	Errores de los usuarios	Datos no adecuados para hacer pruebas
Datos / Información	Datos de configuración	Divulgación de información	Uso sin restricción de medios extraíbles e internet
Datos / Información	Datos de configuración	Errores de configuración	Falta de conocimiento adecuado

Tipo de Activo	Activo	Amenaza	Vulnerabilidad
Software	Ofimática	Alteración accidental de la información	No se tiene versionamiento de los documentos
Software	Visual Studio	Errores de los usuarios	Interfaz de usuario compleja
Software	Visual Studio	Uso no previsto	No se tiene control sobre el uso del software
Software	Visual Studio	Manipulación de programas	Asignación de usuario administrador de equipo
Software	Motor Base Datos	Divulgación de información	Asignación errada de los derechos de acceso
Software	Motor Base Datos	Abuso de privilegios de acceso	Asignación errada de los derechos de acceso
Software	Motor Base Datos	Uso no previsto	No se tiene control sobre el uso del software
Software	Motor Base Datos	Modificación deliberada de información	Ausencia de logs de auditoria
Software	Team Foundation Server	Errores de los usuarios (Desarrolladores)	Interfaz de usuario compleja
Software	Team Foundation Server	Errores del administrador	Múltiples ramas de desarrollo en el programa son administradas por una sola persona
Software	Team Foundation Server	Abuso de privilegios de acceso	Inadecuada gestión de permisos
Software	Team Foundation Server	Divulgación de información	Inadecuada gestión de permisos
Software	Antivirus	Errores del administrador	Algunos equipos no tienen correctamente configurado el antivirus
Software	Antivirus	Difusión de software dañino	Antivirus no se actualiza periódicamente

Tipo de Activo	Activo	Amenaza	Vulnerabilidad
Software	Antivirus	Manipulación de programas	Antivirus puede ser desactivado por el usuario
Software	Internet Information Services	Divulgación de información	Inadecuada configuración permite explorar directorios no autorizados
Software	Aplicaciones internas	Manipulación de programas	Código fuente de aplicaciones internas está a disposición de todos los desarrolladores
Hardware	Laptops	Desastres naturales	Oficina ubicada en zona susceptible a desastre natural
Hardware	Laptops	Fuego	Equipo susceptible de ser destruido por incendio
Hardware	Laptops	Avería de origen físico o lógico	Equipo susceptible a avería de hardware por funcionamiento cotidiano
Hardware	Laptops	Errores de mantenimiento / actualización de equipos	Ausencia de programa de mantenimiento técnico y reemplazo de equipos
Hardware	Laptops	Pérdida de equipos	Ausencia de programa de mantenimiento técnico y reemplazo de equipos
Hardware	Laptops	Abuso de privilegios de acceso	Inadecuada gestión de permisos de usuario
Hardware	Laptops	Uso no previsto	No se tiene control sobre el uso del equipo
Hardware	Laptops	Robo	Equipos se pueden sacar de oficina por visita a cliente o trabajo desde casa
Hardware	Servidor interno	Desastres naturales	Oficina ubicada en zona susceptible a desastre natural
Hardware	Servidor interno	Fuego	Equipo susceptible de ser destruido por incendio

Tipo de Activo	Activo	Amenaza	Vulnerabilidad
Hardware	Servidor interno	Avería de origen físico o lógico	Equipo susceptible a averia de hardware por funcionamiento cotidiano
Hardware	Servidor interno	Errores de mantenimiento / actualización de equipos	Ausencia de programa de mantenimiento técnico y reemplazo de equipos
Hardware	Servidor interno	Pérdida de equipos	Ausencia de programa de mantenimiento técnico y reemplazo de equipos
Hardware	Servidor interno	Abuso de privilegios de acceso	Inadecuada gestión de permisos de usuario
Hardware	Servidor interno	Uso no previsto	No se tiene control sobre el uso del equipo
Hardware	Servidor interno	Corte de suministro electrico	Equipo puede ser afectado por variaciones de voltaje
Hardware	Servidor virtual Pruebas	Avería de origen físico o lógico	Equipo susceptible a averia de origen lógico por funcionamiento cotidiano
Hardware	Servidor virtual Pruebas	Errores de mantenimiento / actualización de equipos	Equipo susceptible a fallas en el procedimiento de actualización de software
Hardware	Servidor virtual Pruebas	Caídas del sistema por agotamiento de recursos	Equipo es usado para múltiples pruebas, por lo que puede tener un exceso de uso de recursos
Hardware	Servidor virtual Pruebas	Uso no previsto	No se tiene control sobre el uso del equipo
Hardware	Router	Desastres naturales	Oficina ubicada en zona susceptible a desastre natural
Hardware	Router	Fuego	Equipo susceptible de ser destruido por incendio
Hardware	Router	Avería de origen físico o lógico	Equipo susceptible a avería de hardware o software

Tipo de Activo	Activo	Amenaza	Vulnerabilidad
Hardware	Router	Corte de suministro eléctrico	Equipo puede ser afectado por variaciones de voltaje
Hardware	Firewall	Desastres naturales	Oficina ubicada en zona susceptible a desastre natural
Hardware	Firewall	Fuego	Equipo susceptible de ser destruido por incendio
Hardware	Firewall	Avería de origen físico o lógico	Equipo susceptible a avería de hardware o software
Hardware	Firewall	Corte de suministro eléctrico	Equipo puede ser afectado por variaciones de voltaje
Soportes de información	Disco externo	Desastres naturales	Oficina ubicada en zona susceptible a desastre natural
Soportes de información	Disco externo	Fuego	Equipo susceptible de ser destruido por incendio
Soportes de información	Disco externo	Avería de origen físico o lógico	Equipo susceptible a avería de hardware o software
Soportes de información	Disco externo	Corte de suministro eléctrico	Equipo puede ser afectado por variaciones de voltaje
Soportes de información	Disco externo	Uso no previsto	No se tiene control sobre el uso del equipo
Redes de comunicaciones	Internet	Fallo de servicios de comunicaciones	Se tiene un solo proveedor de servicio sin enlace de backup
Redes de comunicaciones	Internet	Fugas de información	Existe libre uso de correo y chat personal
Redes de comunicaciones	Internet	Uso no previsto	Existe libertad de acceso a cualquier página web
Redes de comunicaciones	Internet	Análisis de tráfico	Red es susceptible a monitorización de tráfico

Tipo de Activo	Activo	Amenaza	Vulnerabilidad
Redes de comunicaciones	Internet	Interceptación de información	Red es susceptible a análisis de tráfico
Redes de comunicaciones	Internet	Divulgación de información	Existe libre uso de correo y chat personal
Redes de comunicaciones	Red local	Abuso de privilegios de acceso	Protección inadecuada para acceso de terceros
Redes de comunicaciones	Red local	Análisis de tráfico	Protección inadecuada para acceso de terceros
Redes de comunicaciones	Red local	Interceptación de información	Protección inadecuada para acceso de terceros
Instalaciones	Oficina	Desastres naturales	Oficina ubicada en zona susceptible a desastre natural
Instalaciones	Oficina	Fuego	Oficina queda cerca de gasolinera
Instalaciones	Oficina	Desastres industriales	Edificio donde se encuentra oficina es antiguo
Personal	Desarrollador	Deficiencias en la organización	No se tiene claro los procedimientos ante un incidente de seguridad
Personal	Desarrollador	Indisponibilidad del personal	En ciertas tareas existe solo una persona que puede realizarla
Personal	Desarrollador	Ingeniería Social	Intento por parte de terceros de beneficiarse de información de proyectos
Personal	Desarrollador	Fugas de información	Divulgación accidental de información sensible del proyecto asignado
Personal	Jefe de Proyecto	Deficiencias en la organización	No se tiene claro los procedimientos ante un incidente de seguridad
Personal	Jefe de Proyecto	Indisponibilidad del personal	En caso de ausencia, no hay control sobre los proyectos

Tipo de Activo	Activo	Amenaza	Vulnerabilidad
Personal	Jefe de Proyecto	Ingenieria Social	Intento por parte de terceros de beneficiarse de información de proyectos
Personal	Jefe de Proyecto	Fugas de información	Divulgación accidental de información sensible del proyecto asignado
Personal	Usuario de prueba	Fugas de información	Divulgación accidental de información sensible del proyecto asignado

3.6 ANÁLISIS DE RIESGOS

En el caso de que una amenaza identificada se materialice, la afectación sobre el valor de un activo se conoce como degradación. Esta degradación es un porcentaje de pérdida de valor del activo, aunque en algunos casos cuando hay una amenaza intencional, es difícil estimar el daño causado con valores numéricos. Para estos casos se puede hacer uso de tablas para el análisis cualitativo lo que permite sin entrar en tanto detalle identificar los riesgos más críticos a ser tratados.

Para representar el impacto sobre un activo se ha usado la siguiente escala:

Tabla 8. Impacto de los riesgos sobre los activos

Impacto		Descripción
Muy Alto	MA	Consecuencias desastrosas
Alto	A	Consecuencias importantes
Medio	M	Consecuencias de mediana importancia
Bajo	B	Bajo impacto sobre entidad
Muy Bajo	MB	Efectos mínimos

Teniendo el valor del activo y una estimación de la degradación en caso de amenaza, para estimar el impacto, se ha realizado un análisis como se indica en la Tabla 9.

Tabla 9. Impacto a partir de la valoración y la degradación de activos

IMPACTO		Degradación de activo		
		Baja	Media	Alta
Valoración de activo	Muy Alta	M	A	MA
	Alta	B	M	A
	Media	MB	B	M
	Baja	MB	MB	B
	Muy Baja	MB	MB	MB

Para la probabilidad se ha hecho uso de la siguiente escala:

Tabla 10. Escala de probabilidad de ocurrencia de una amenaza

Probabilidad de ocurrencia		**Descripción**
Muy Alta	MA	Casi seguro, ocurre muy frecuentemente
Alta	A	Ocurrencia frecuente
Media	M	Es posible que suceda
Baja	B	Baja probabilidad, poco frecuente
Muy Raro	MR	Muy difícil que ocurra

El cálculo de riesgos es resultado de la combinación la probabilidad de que se produzca un incidente de seguridad y el impacto sobre la entidad afectado.

Tabla 11. Riesgo en función de Probabilidad e Impacto

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 12. Matriz de Riesgos

Código	Activo	Amenaza	Valor activo	Degradación	Impacto	Probabilidad	Riesgo
DI001	Documentación	Alteración accidental de la información	A	A	A	M	A
DI001	Documentación	Modificación deliberada de información	A	A	A	M	A
DI001	Documentación	Destrucción de la información	A	A	A	B	A
DI001	Documentación	Divulgación de información	A	M	B	B	B
DI002	Código fuente	Alteración accidental de la información	MA	A	MA	A	MA
DI002	Código fuente	Destrucción de la información	MA	A	MA	B	MA
DI002	Código fuente	Divulgación de información	MA	A	MA	M	MA
DI003	Manuales	Destrucción de la información	M	A	M	B	M
DI003	Manuales	Divulgación de información	M	B	B	B	B
DI004	Datos de prueba	Errores de los usuarios	M	B	B	M	B
DI005	Datos de configuración	Divulgación de información	M	M	B	B	B
DI005	Datos de configuración	Errores de configuración	M	A	M	M	M
SO001	Ofimática	Alteración accidental de la información	B	A	B	B	B
SO002	Visual Studio	Errores de los usuarios	A	B	B	B	B
SO002	Visual Studio	Uso no previsto	A	B	B	B	B
SO002	Visual Studio	Manipulación de programas	A	B	B	M	B
SO003	Motor Base Datos	Divulgación de información	A	A	A	M	A

Código	Activo	Amenaza	Valor activo	Degradación	Impacto	Probabilidad	Riesgo
SO003	Motor Base Datos	Abuso de privilegios de acceso	A	A	A	M	A
SO003	Motor Base Datos	Uso no previsto	A	M	B	M	B
SO003	Motor Base Datos	Modificación deliberada de información	A	A	A	B	A
SO004	Team Foundation Server	Errores de los usuarios (Desarrolladores)	A	B	B	A	M
SO004	Team Foundation Server	Errores del administrador	A	B	B	M	B
SO004	Team Foundation Server	Abuso de privilegios de acceso	A	A	A	B	A
SO004	Team Foundation Server	Divulgación de información	A	M	B	M	B
SO005	Antivirus	Errores del administrador	MB	A	MB	B	MB
SO005	Antivirus	Difusión de software dañino	MB	A	MB	B	MB
SO005	Antivirus	Manipulación de programas	MB	M	MB	MR	MB
SO006	Internet Information Server	Divulgación de información	B	M	MB	B	MB
SO007	Aplicaciones internas	Manipulación de programas	M	M	B	B	B
HA001	Laptops	Desastres naturales	A	A	A	MR	M
HA001	Laptops	Fuego	A	A	A	MR	M
HA001	Laptops	Avería de origen físico o lógico	A	A	A	M	A
HA001	Laptops	Errores de mantenimiento /	A	M	B	A	M

Código	Activo	Amenaza	Valor activo	Degradación	Impacto	Probabilidad	Riesgo
		actualización de equipos					
HA001	Laptops	Pérdida de equipos	A	A	A	MR	M
HA001	Laptops	Abuso de privilegios de acceso	A	A	A	MR	M
HA001	Laptops	Uso no previsto	A	M	B	M	B
HA001	Laptops	Robo	A	A	A	MR	M
HA002	Servidor interno	Desastres naturales	A	A	A	MR	M
HA002	Servidor interno	Fuego	A	A	A	MR	M
HA002	Servidor interno	Avería de origen físico o lógico	A	A	A	MR	M
HA002	Servidor interno	Errores de mantenimiento / actualización de equipos	A	A	A	M	A
HA002	Servidor interno	Pérdida de equipos	A	A	A	MR	M
HA002	Servidor interno	Abuso de privilegios de acceso	A	A	A	MR	M
HA002	Servidor interno	Uso no previsto	A	M	B	B	B
HA002	Servidor interno	Corte de suministro electrico	A	M	B	M	B
HA003	Servidor virtual Pruebas	Avería de origen físico o lógico	A	M	B	M	B
HA003	Servidor virtual Pruebas	Errores de mantenimiento / actualización de equipos	A	M	B	M	B
HA003	Servidor virtual Pruebas	Caidas del sistema por agotamiento de recursos	A	M	B	B	B
HA003	Servidor virtual Pruebas	Uso no previsto	A	B	B	M	B
HA004	Router	Desastres naturales	M	A	M	MR	B
HA004	Router	Fuego	M	A	M	MR	B

Código	Activo	Amenaza	Valor activo	Degradación	Impacto	Probabilidad	Riesgo
HA004	Router	Avería de origen físico o lógico	M	A	M	B	M
HA004	Router	Corte de suministro electrico	M	B	B	B	B
HA005	Firewall	Desastres naturales	M	A	M	MR	B
HA005	Firewall	Fuego	M	A	M	MR	B
HA005	Firewall	Avería de origen físico o lógico	M	A	M	B	M
HA005	Firewall	Corte de suministro electrico	M	B	B	B	B
SI001	Disco externo	Desastres naturales	M	A	M	MR	B
SI001	Disco externo	Fuego	M	A	M	MR	B
SI001	Disco externo	Avería de origen físico o lógico	M	A	M	M	M
SI001	Disco externo	Corte de suministro electrico	M	B	B	B	B
SI001	Disco externo	Uso no previsto	M	M	B	M	B
CO001	Internet	Fallo de servicios de comunicaciones	M	A	M	M	M
CO001	Internet	Fugas de información	M	A	M	B	M
CO001	Internet	Uso no previsto	M	N	B	M	B
CO001	Internet	Análisis de tráfico	M	A	M	B	M
CO001	Internet	Interceptación de información	M	A	M	B	M
CO001	Internet	Divulgación de información	M	A	M	B	M
CO002	Red local	Abuso de privilegios de acceso	M	A	M	B	M
CO002	Red local	Análisis de tráfico	M	A	M	B	M
CO002	Red local	Interceptación de información	M	A	M	B	M
IN001	Oficina	Desastres naturales	M	A	M	MR	B
IN001	Oficina	Fuego	M	A	M	MR	B

Código	Activo	Amenaza	Valor activo	Degradación	Impacto	Probabilidad	Riesgo
PE001	Desarrollador	Deficiencias en la organización	M	A	M	A	A
PE001	Desarrollador	Indisponibilidad del personal	M	A	M	M	M
PE001	Desarrollador	Ingenieria Social	M	M	B	M	B
PE001	Desarrollador	Fugas de información	M	A	M	A	A
PE002	Jefe de Proyecto	Deficiencias en la organización	M	A	M	M	M
PE002	Jefe de Proyecto	Indisponibilidad del personal	M	A	M	M	M
PE002	Jefe de Proyecto	Ingenieria Social	M	M	B	MR	MB
PE002	Jefe de Proyecto	Fugas de información	M	A	M	B	M
PE003	Usuario de prueba	Fugas de información	MB	M	MB	M	MB

A partir de la información mostraba en la tabla 12 se puede verificar que los activos con mayor nivel de riesgo son:

- *Código fuente.* Es el activo de información con más alto valor para el proceso y el que al ser vulnerada su seguridad puede haber consecuencias muy serias para la empresa. Esto ocurre debido a que es el producto del desarrollo de sistemas, pero esta al acceso de cualquier persona con una laptop en la red de la empresa. Un ataque a su seguridad puede causar graves perjuicios económicos comprometiendo confidencialidad, disponibilidad e integridad además

de la reputación y la propiedad intelectual de la empresa. La única medida implementada es el respaldo de información propio del uso de un sistema de control de versiones como lo es el Team Foundation Server.

- *Documentación*. Este activo es de alto valor para la empresa porque es donde reside los requerimientos antes de la programación de los sistemas. Son la base para la planificación de proyectos, contienen información confidencial de los procesos de los clientes. Por lo tanto, la vulneración de su seguridad implica un impacto directo al proceso estudiado en este análisis. La documentación se encuentra en el servidor interno en una carpeta común sin medidas de protección ante personal que esté en la red de la empresa.
- *Motor de Base de Datos*. Una vulneración a su seguridad afectaría a la disponibilidad de bases de datos para las pruebas de los sistemas además de posiblemente verse afectada la confidencialidad de la información y la integridad en sí de los sistemas.
- *Team Foundation Server*. Es el sistema de control de código fuente. En este reside toda la historia de cambios por lo que un ataque a su seguridad afecta la integridad del código de las aplicaciones. El único control existente es que existen permisos requeridos para manipular el código de funcionalidades listas para producción mientras que todos tienen acceso el código de las funcionalidades en desarrollo.

- *Laptops*. La no disponibilidad de este activo impide que actividades a ser cumplidas por los desarrolladores se cumplan. Existen medidas para el mantenimiento de hardware, pero no son formales.
- *Desarrolladores*. La no disponibilidad impide que las actividades del proceso se cumplan. Para ciertas actividades solo hay una persona especializada. Además, ante un incidente de seguridad no conocen que procedimientos seguir.

3.7 PLAN DE TRATAMIENTO DE RIESGOS

El propósito del análisis de riesgos es conocer lo que se desea proteger y el riesgo al que está sometido. A partir de la información mostrada en la Tabla 12, la gerencia de la empresa considera que no se puede optar por la eliminación de ningún riesgo ya que esto se logra mediante la eliminación de los activos de información lo cual no es posible. Los riesgos con valor muy bajo, bajo o medio han sido aceptados. Mientras que para los riesgos con valor alto o muy alto la gerencia ha decidido seleccionar una de las opciones de tratamiento que son mitigación mediante la implementación de controles o la transferencia de los riesgos. Para seleccionar los controles se ha seleccionado de lo propuesto por la norma ISO/IEC 27002:2013.

Tabla 13. Plan de tratamiento de riesgos

	Activo	Amenaza	Impacto	Probabilidad	Riesgo	Tratamiento	Responsable	Control / Actividad	Impacto	Probabilidad	Riesgo
R1	Documentación	Alteración accidental de la información	A	M	A	Mitigar	Oficial seguridad información	9.1.1 Política de control de acceso 12.1.1 Documentación de procedimientos de operación 12.3.1 Respaldo de la información	B	B	B
R2	Documentación	Modificación deliberada de información	A	M	A	Mitigar	Oficial seguridad información	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información 13.2.1 Políticas y procedimientos de intercambio de información 18.1.3 Protección de los registros de la organización	B	B	B
R3	Documentación	Destrucción de la información	A	B	A	Mitigar	Oficial seguridad información	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información 13.2.1 Políticas y procedimientos de intercambio de información 18.1.3 Protección de los registros de la organización	M	B	M
R4	Código fuente	Alteración accidental de la información	MA	A	MA	Mitigar	Jefe de desarrollo	9.1.1 Política de control de acceso 12.1.1 Documentación de procedimientos de operación 12.3.1 Respaldo de la información	M	B	M

	Activo	Amenaza	Impacto	Probabilidad	Riesgo	Tratamiento	Responsable	Control / Actividad	Impacto	Probabilidad	Riesgo
R5	Código fuente	Destrucción de la información	MA	B	MA	Mitigar	Jefe de desarrollo	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información 13.2.1 Políticas y procedimientos de intercambio de información 18.1.3 Protección de los registros de la organización	M	B	M
R6	Código fuente	Divulgación de información	MA	M	MA	Mitigar	Jefe de desarrollo	13.2.4 Acuerdos de confidencialidad	MA	MR	A
R7	Motor Base Datos	Divulgación de información	A	M	A	Mitigar	Oficial seguridad información	13.2.4 Acuerdos de confidencialidad	A	MR	M
R8	Motor Base Datos	Abuso de privilegios de acceso	A	M	A	Mitigar	Oficial seguridad información	9.2.5 Revisión de los derechos de acceso de los usuarios	A	MR	M
R9	Motor Base Datos	Modificación deliberada de información	A	B	A	Mitigar	Analista de sistemas	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información 13.2.1 Políticas y procedimientos de intercambio de información 18.1.3 Protección de los registros de la organización	M	B	M
R10	Team Foundation Server	Abuso de privilegios de acceso	A	B	A	Mitigar	Oficial seguridad información	9.2.5 Revisión de los derechos de acceso de los usuarios	A	MR	M

	Activo	Amenaza	Impacto	Probabilidad	Riesgo	Tratamiento	Responsable	Control / Actividad	Impacto	Probabilidad	Riesgo
R11	Laptops	Avería de origen físico o lógico	A	M	A	Mitigar	Analista de sistemas	8.1.3 Uso aceptable de los activos 12.6.1 Gestión de las vulnerabilidades técnicas 12.6.2 Restricción en la instalación de software	M	MR	B
R12	Laptops	Errores de mantenimiento / actualización de equipos	M	A	A	Mitigar	Analista de sistemas	11.2.4 Mantenimiento de los equipos	M	MR	B
R13	Desarrollador	Deficiencias en la organización	M	A	A	Mitigar	Jefe de proyectos	6.1.1 Roles y responsabilidades para la seguridad de información 6.1.2 Separación de tareas 7.2.2 Toma de conciencia, educación y capacitación en seguridad	M	MR	B
R14	Desarrollador	Fugas de información	M	A	A	Mitigar	Oficial seguridad información	6.1.1 Roles y responsabilidades para la seguridad de información 6.1.2 Separación de tareas 7.2.2 Toma de conciencia, educación y capacitación en seguridad de información en seguridad	M	MR	B

Los riesgos antes de aplicarse controles para mitigar su impacto son conocidos como riesgos inherentes.

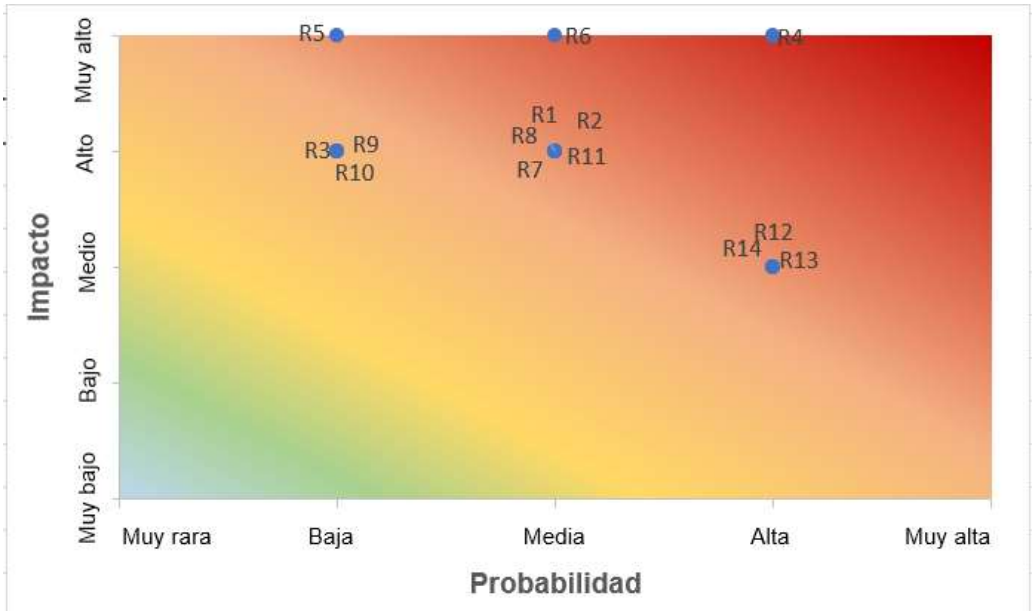

Figura 4.1. Mapa de calor de Riesgos Inherentes

Fuente: Autor

Una vez se ha aplicado los controles, los riesgos que se mantienen son conocidos como riesgos residuales. Como se puede observar, los riesgos residuales se mantienen en niveles entre medio a bajo.

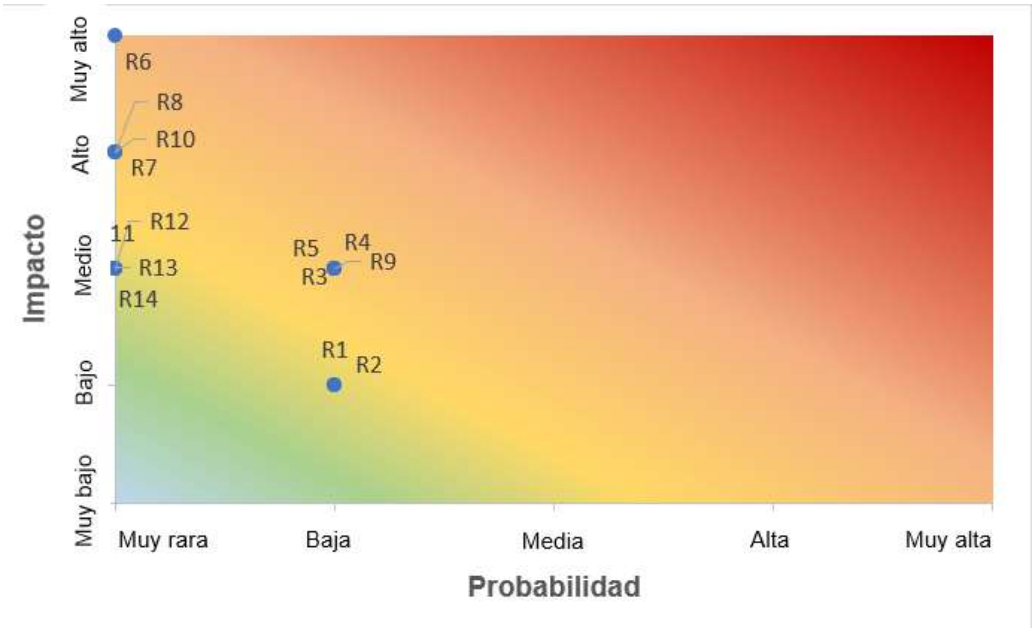

Figura 4.2 Mapa de calor de riesgos residuales

Fuente: Autor

CAPÍTULO 4

DESARROLLO Y PRUEBAS

4.1 DEFINICIÓN DE LOS PROYECTOS DEL PLAN DE TRATAMIENTO DE RIESGOS

Una vez identificados los controles necesarios para reducir los riesgos más críticos se ha procedido a definir los proyectos para implementarlos.

Para estimar los costos financieros se ha un cálculo en base al tiempo dedicado por los responsables asignados al proyecto.

Proyecto 1	Mantenimiento y configuración de equipos
Responsable	Sistemas
Tiempo aproximado	1 mes
Recursos	$1000

Objetivo

Revisar la configuración de los equipos usados por el personal de desarrollo, instalar programas de protección contra malware, hacer actualizaciones.

Controles a implementar

11.2.4 Mantenimiento de equipos

12.2.1 Controles para el código malicioso

12.6.2 Restricción en la instalación de software

Proyecto 2	Creación de políticas de seguridad
Responsables	Oficial de seguridad de información Jefe de desarrollo, Jefe de proyectos
Tiempo aproximado	3 meses
Recursos	Total: $2880

Objetivo

Crear la documentación necesaria para cumplir con los controles de seguridad necesarios.

Controles a implementar

6.1.1 Roles y responsabilidades para la seguridad de información

6.1.2 Separación de tareas

8.1.3 Uso aceptable de los activos

9.1.1 Política de control de acceso

12.1.1 Documentación de procedimientos de operación

12.3.1 Respaldo de la información

12.6.1 Gestión de las vulnerabilidades técnicas

13.2.1 Políticas y procedimientos de intercambio de información

13.2.4 Acuerdos de confidencialidad

Proyecto 3	Capacitación al personal
Responsable	Oficial de seguridad de información
Tiempo aproximado	1 mes
Recursos	$500
Objetivo Capacitar al personal de la empresa en políticas relacionadas con la seguridad de información y la respuesta ante incidentes de seguridad. *Controles a implementar* 7.2.2 Toma de conciencia, educación y capacitación en seguridad de información	

Proyecto 4	Revisión de accesos
Responsables	Sistemas
Tiempo aproximado	5 días
Recursos	Total: $100
Objetivo Revisar los derechos de acceso a los usuarios. *Controles a implementar* 9.2.5 Revisión de los derechos de acceso de usuario	

Proyecto 5	Protección de los registros de la organización
Responsables	Sistemas Oficial de seguridad de información
Tiempo aproximado	1 mes
Recursos	$500
Objetivo Proteger los registros contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados. *Controles a implementar* 18.1.3 Protección de los registros de la organización	

4.2 DESARROLLO DE LOS PROYECTOS DEL PLAN DE TRATAMIENTO DE RIESGOS

Proyecto 1. Mantenimiento y configuración de equipos.

En este proyecto se han definido tareas técnicas que pueden ser ejecutadas de manera inmediata. Están a cargo del Analista de sistemas.

Las tareas realizadas son:

1. Actualizar inventario de activos. Al momento de recibir los activos para trabajar se verifica que la información esté correcta en el inventario.
2. Actualizar programas y sistema operativo. Se actualiza todos los programas que necesitan los desarrolladores y se remueven los instalados que no tengan que ver con su trabajo. Los programas usados por los desarrolladores son SQL Server, Visual Studio, Git, Ofimática y los sistemas internos que defina la alta dirección.
3. Restringir permisos de instalación de programa. Se les asigna un usuario Windows en la laptop que le corresponde a cada desarrollador que no permita instalar programas adicionales sin autorización.

Mediante la ejecución de estas actividades se espera que baje la probabilidad de ocurrencia de averías en los equipos.

Proyecto 2. Creación de políticas de seguridad

En este proyecto se realizarán actividades para la creación de políticas de seguridad. Una política de seguridad de información es un documento con las reglas que se debe seguir en la empresa. Cada política usualmente tiene las siguientes secciones:

- Introducción
- Propósito
- Alcance

- Enunciados de la política
- Sanciones
- Glosario
- Fecha de publicación
- Versión del documento
- Referencias

Las políticas que se ha propuesto de acuerdo a los controles necesarios son:

- Política de respaldo de información.
- Política de uso aceptable de activos
- Política de mantenimiento de equipos
- Política de protección de la información
- Política de correo

Mediante la creación de las políticas de seguridad mencionadas se espera disminuir tanto la probabilidad como el impacto de los riesgos asociados principalmente a los datos e información importante de la empresa.

Proyecto 3. Capacitación al personal

En este proyecto se han planificado las capacitaciones que estarán basadas en dar a conocer y despejar dudas acerca de las políticas de seguridad de información implementadas.

Mediante capacitación al personal se espera que se disminuya la probabilidad de ocurrencia de riesgos asociados a fugas de información o de no saber como actuar ante un incidente de seguridad.

Proyecto 4. Revisión de accesos

A cargo del Analista de sistemas, este proyecto tiene como objetivo verificar que los accesos a los usuarios que hacen uso de las instalaciones y equipos de la empresa tengan una configuración de acceso adecuada de acuerdo con sus niveles de acceso.

Al realizar esta revisión, se disminuye la probabilidad de que ocurre un incidente relacionado con el abuso de privilegios.

Proyecto 5. Protección de los registros de la organización

En este proyecto se tiene como objetivo proteger los registros de información mas importantes. Lo que se debe proteger y como hacerlo es de responsabilidad del oficial de seguridad de información luego de haberse reunido con la gerencia y los jefes de desarrollo y proyectos para establecer cual es la información que amerita un nivel adicional de protección. Cambios de rutas de carpetas, cifrado de archivos y otras técnicas pueden ser usadas.

Con la ejecución de estas actividades se espera disminuir tanto la probabilidad como el impacto de los riesgos que puedan afectar la confidencialidad e integridad de la información.

Los proyectos están planificados para realizarse en un periodo de tres meses como se muestra a continuación en la Figura 7:

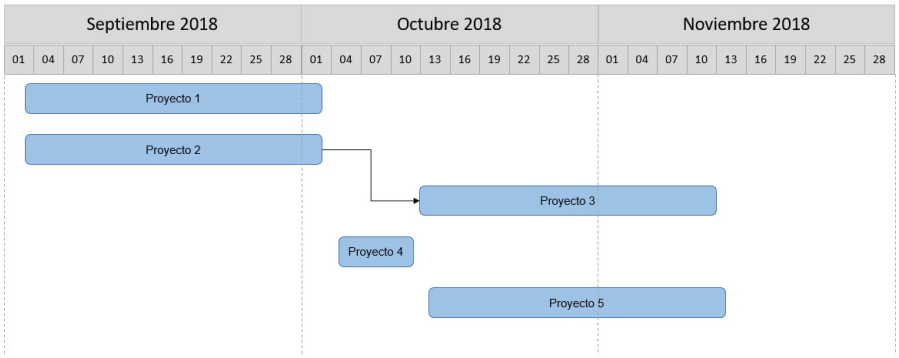

Figura 5.1 Plan de implementación de tratamiento de riesgo

Fuente. El Autor

4.3 PRUEBAS DEL PLAN DE TRATAMIENTO DE RIESGOS

En el caso de que suceda uno de los riesgos detectados es importante verificar la eficacia de los controles propuestos en el plan de tratamiento se ha planteado los siguientes escenarios de prueba:

Escenario de prueba 1

Mientras se está haciendo uso de una laptop para el desarrollo de una tarea asignada con fecha límite establecida, la laptop se apaga y no vuelve

a encender. Esto afecta la ejecución normal de las actividades y un posible desplazamiento en el cronograma de desarrollo de sistemas generando costos adicionales a la empresa.

Amenazas: Destrucción de la información, Avería de origen físico o lógico

Activos afectados: Documentación, código fuente, laptop

Escenario de prueba 2

Un empleado sospecha que será removido de su cargo y planea copiar el código fuente del ERP que está desarrollando para usarlo en una extorsión a la empresa y así obtener un beneficio económico. En caso de no obtener lo que solicita, amenaza con la divulgación de código cerrado a través de internet. Esto atenta contra la propiedad intelectual de la empresa y una posible pérdida de oportunidades comerciales.

Amenazas: Deficiencias en la organización, abuso de privilegios de acceso, divulgación de información.

Activos afectados: Código fuente

Escenario de prueba 3

Un software malicioso infecta una de las laptops usadas por un desarrollador con una tarea crítica en el módulo en desarrollo. Este software malicioso cual termina encriptando los datos del equipo y

pidiendo un pago en una criptomoneda para poder desencriptar los datos. Esto impide la normal ejecución de las actividades del desarrollador.

Amenazas: Destrucción de la información, Avería de origen físico o lógico

Activos afectados: Documentación, código fuente, base de datos

CAPÍTULO 5

ANÁLISIS DE RESULTADOS

5.1 REVISIÓN DE LOS RESULTADOS DE LAS PRUEBAS

Para cada uno de los escenarios propuestos, se han encontrado los siguientes resultados:

Escenario de prueba 1

Para este escenario, existen los controles documentados, aunque su ejecución es manual. Para disminuir el riesgo de que exista una avería en la laptop se ha propuesto un plan de manteamiento de equipos y políticas de uso aceptable de activos. Para evitar la pérdida de información existe una política de respaldo de información. El responsable de la ejecución de estos controles es al Analista de Sistemas.

Escenario de prueba 2

El caso de copia de código fuente puede tener un gran impacto sobre la empresa ya que es uno de los activos más importantes que tiene. En el caso de que un empleado decida irse en malos términos existe un Acuerdo de Confidencialidad el cual debe ser firmado por cualquier persona que ingresa a trabajar a la empresa. Así mismo, mientras labora a la compañía solo tendrá acceso al código fuente de la tarea asignada y lo mínimo necesario para probar el sistema en el que trabaja.

Escenario de prueba 3

Existe un control para reducir el riesgo de infección de una o varias máquinas. En el momento que se dé una infección de malware al sistema operativo, existe una política documentada de los pasos a seguir. Y en el

caso de que no se pueda recuperar la información, existe un a política de respaldo de información por lo que se podría recuperar en parte la información pérdida.

5.2 IMPACTO EN LOS INTERESADOS

Para la gerencia de la empresa, la implementación de controles ha sido un reto ya que no había una cultura orientada a la seguridad de información sino a la satisfacción de necesidades de los clientes lo mas pronto posible.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Se ha realizado un estudio orientado a encontrar los riesgos de seguridad de información del proceso de desarrollo de sistemas para tratarlos de una manera adecuada del cual podemos concluir lo siguiente:

1. A partir del análisis de riesgo realizado se ha entendido el valor de ciertos activos de información y el impacto que causaría una amenaza materializada para el proceso de desarrollo. Al ser el resultado del

trabajo intelectual del equipo humano que labora en la empresa, el código fuente es considerado el activo de información de mayor valor desde el punto de vista de la seguridad de información. Ataques a la disponibilidad de los programas usados por los desarrolladores o a la documentación en la que se basan para sus actividades diarias también tiene una alta valoración. El hardware usado para programar y para hacer pruebas también es critico que se encuentre protegido ya que si falla su seguridad entonces el proceso no puede continuar con normalidad.

2. Al evaluar los riesgos de seguridad sobre los activos más críticos para el proceso se ha encontrado que los que involucran errores humanos son los que mayor probabilidad tienen de ocurrir mientras que una modificación o divulgación de información no intencional ni autorizada es lo que mas causaría impacto. También causaría bastante impacto una pérdida del medio de trabajo de los desarrolladores como lo son las laptops.
3. Se ha desarrollado un plan de tratamiento de riesgos partiendo de los controles propuestos por la norma ISO/IEC 27002:2013, proponiendo proyectos que buscan implementar uno o varios de estos controles.

RECOMENDACIONES

La gestión de riesgos es un proceso que se debe realizar continuamente ya que, aunque se reduzcan ciertos riesgos, con el tiempo puede ser que cambien las amenazas detectadas o incluso pueden aparecer nuevas amenazas. Entre las actividades que pueden realizarse para mejorar continuamente la seguridad de información del proceso de desarrollo de sistemas y de los demás procesos en la empresa están:

1. Mantener actualizado el inventario de activos de información y asignar un responsable de la seguridad de cada uno de ellos.
2. Capacitar al personal continuamente en como reaccionar ante incidentes de seguridad que afecten la confidencialidad y la integridad de la información sensible para la empresa.
3. Optimizar los procedimientos de mantenimiento de hardware y software para reducir al máximo la no disponibilidad en el proceso de desarrollo.
4. Incluir en el proceso de desarrollo de sistemas un especialista en seguridad que les ayude a los desarrolladores no solo a mantener el proceso de desarrollo seguro, sino que también a hacer sistemas de información seguros lo cual incrementará la confianza de los clientes en los productos y servicios proporcionados por la empresa.

BIBLIOGRAFÍA

[1] ESET, Tendencias en ciberseguridad 2018: El costo de nuestro mundo conectado, https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf, fecha de consulta Septiembre de 2018

[2] Cano, Jeimy J., JOnline: La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes, https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx, fecha de consulta Julio de 2018

[3] ISOTools Excellence, Los tres pilares de la seguridad de la información, https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad, fecha de consulta Julio de 2018

[4] Policia Nacional del Ecuador, Los activos de la seguridad de la información y sus riesgos, http://www.policiaecuador.gob.ec/los-activos-de-la-seguridad-de-la-informacion-y-sus-riesgos, fecha de consulta Agosto de 2018

[5] Instituto Nacional de Ciberseguridad de España, Gestión de riesgos. Una guia de aproximación para el empresario,

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf, fecha de consulta Septiembre de 2018

[6] Benjumea, Omar, ¿Sabes diferenciar la ISO 27001 y la ISO 27002?, http://www.redseguridad.com/especialidades-tic/certificaciones-y-formacion/sabes-diferenciar-la-iso-27001-y-la-iso-27002, fecha de consulta Julio de 2018

[7] ISOTools Excellence, La norma ISO 27002 complemento para la ISO 27001, https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001, fecha de consulta Julio de 2018

[8] Portal de Administración Electrónica del Gobierno de España, MAGERIT v.3:Metodología y Gestión de Riesgos de Sistemas de Información, https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W5ciOgzZPY, fecha de consulta Agosto de 2018