USMP
UNIVERSIDAD DE SAN MARTIN DE PORRES

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN PROCESOS TECNOLÓGICOS

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

PRESENTADO POR

BARRANTES PORRAS, CARLOS EDUARDO

HUGO HERRERA, JAVIER ROBERTO

LIMA – PERÚ

2012

ÍNDICE

RESUMEN

En la actualidad, muchas empresas que están o desean incursionar en el ámbito financiero tienen problemas para resguardar la seguridad de su información; en consecuencia esta corre riesgos al igual que sus activos.

El propósito de este trabajo se centró en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por los autores de este trabajo, también se usaron como referencias las normas ISO 27001:2005 e ISO 17799:2005.

Esta implementación permitió un gran aumento en la seguridad de los activos de información de la empresa Card Perú S.A., que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Palabras clave: sistema de gestión de seguridad de la información, análisis y evaluación de riesgos, gestión del riesgo, activo de información.

ABSTRACT

Nowadays, many companies that are interested to enter in the financial field have trouble guarding the security of their information, and consequently this is at risk as its assets.

The purpose of this work is focused on the implementation of an Information Security Management System (ISMS), under a methodology of analysis and risk assessment developed and designed by the authors of this paper; in addition, standards ISO 27001:2005 and ISO 17799:2055 were also used as reference.

This implementation allowed a great increase in the security of information assets of the company Card Peru S.A., ensuring that the information security risks are known, assumed, managed and minimized in a documented, systematic, structured, repeatable, efficient and adaptable way; in order to face any possible change in the risks, environment and technology.

Keywords: information security management system, analysis and risk assessment, risk management, information assets.

INTRODUCCIÓN

En la presente tesis, se diseña y desarrolla el modelo para implementar un sistema de gestión de seguridad de información para cualquier tipo de organización y se encuentra ubicado dentro del área temática de industrias de la información y del conocimiento. Para la aplicación del presente trabajo, se trabajará con una empresa real, que por motivos de seguridad de su información, la llamaremos en adelante: Card Perú S.A, la cual es una entidad financiera o entidad emisora de tarjetas de crédito.

La seguridad de información, en términos generales es entendida como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma. Un activo de información es un activo que tiene un determinado valor para la organización, sus operaciones comerciales y su continuidad.

La característica principal de un sistema de gestión de seguridad de información es resguardar la integridad, confidencialidad e integridad de los activos de información en una empresa; lo cual se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implantar los controles necesarios que ayudarán a proteger estos activos.

La problemática principal actual de las empresas que desean incursionar en el ámbito financiero es la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de no tener las medidas necesarias para mitigar estos riesgos puede llevar a la empresa a pérdidas no solo de información, sino también económica.

Es por ello, que Card Perú S.A. se ve en la necesidad de implementar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando requieran los que estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

El presente trabajo consta de cinco capítulos. Ellos son:

En el capítulo I se presenta el planteamiento del problema, los objetivos, la justificación, las limitaciones y la viabilidad del proyecto

El capítulo II muestra el marco teórico, en el que están planteadas las bases teóricas relacionadas con un sistema de gestión de seguridad de la información (SGSI), definiciones de términos básicos que sustentan el desarrollo adecuado del trabajo y antecedentes de la investigación.

En el capítulo III se especifican los materiales, métodos y herramientas utilizadas para el desarrollo del trabajo de investigación. También se define la metodología a emplear, la cual es la resultante de un estudio de distintas metodologías y de la investigación y aporte de los autores de este trabajo de investigación. Adicionalmente este capítulo también contiene la etapa de desarrollo del proyecto, en la cual se muestra el proceso seguido para la realización del mismo.

El capítulo IV está destinado a la presentación de las pruebas y resultados del trabajo de investigación.

El capítulo V aborda la discusión de los resultados a manera de explicación de los mismos, teniendo en cuenta las variables expuestas en los capítulos anteriores.

A partir de los resultados obtenidos se han planteado las conclusiones y recomendaciones pertinentes, y finalmente se consigna la bibliografía utilizada y los anexos respectivos.

CAPÍTULO I
PLANTEAMIENTO DE PROBLEMA

1.1 Problema

1.1.1 Situación problemática

Las organizaciones públicas y privadas día a día generan conocimientos, datos, reportes, actas y material de diferente índole de suma importancia para ellas, lo cual representa toda la información que requieren para su funcionalidad. Esta información en la mayoría de los casos, es almacenada en diferentes medios tanto físicos como electrónicos, además es puesta a disposición del personal que requiere hacer uso de esta información para toma de decisiones, realización de planes, reportes, inventarios, entre otros.

El acceso no autorizado a la información se ha vuelto más fácil debido a los tantos métodos existentes y nuevos para extraer información, esto ha permitido que sea más difícil salvaguardar la información y sus métodos de transmisión; ya sean estos comunicados verbales, archivos, documentos, base de datos, entre otros.

Debido al crecimiento y expansión de Card Perú S.A., entidad emisora de tarjetas de crédito, la probabilidad de que la información sea interceptada, robada y/o modificada por personas inescrupulosas y sin autorización de acceso a esta, ha aumentado exponencialmente. Lo cual resulta peligroso para la organización, ya que mucha de la información fundamental e importante para la realización de los procesos críticos del negocio puede ser vulnerada y amenazada ocasionando la interrupción de estos procesos; que conllevan, de esta manera, a una pérdida no solo de información, sino también financiera.

Por lo anteriormente citado es necesaria la implementación de herramientas, procedimientos, controles y políticas que aseguren la

confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que accedan a la información quienes estén designados para su uso, esté disponible cuando se requiera y permanezca tal como fue creada por sus propietarios y asegurar también la actualización de la misma.

1.1.2 Definición del problema

Actualmente Card Perú S.A. no cuenta con los controles, medidas, procedimientos de seguridad necesarios para resguardar sus activos de información, tales como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios, están expuestos a altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes:

- Desastres naturales (Tormentas, rayos, terremotos, inundaciones, etc)
- Estructurales (Incendios, inundaciones, humedad, cortes de electricidad, agua, refrigeración, comunicaciones, etc)
- Hardware (Fallo total o parcial de Servidores, Estaciones PC, portátiles, etc)
- Software (Errores en los SO, BD, software base, Web servers, aplicaciones, elementos de seguridad, etc)
- Red LAN y WAN (red interna, redes con delegaciones, sistemas de seguridad de las comunicaciones, redes públicas ajenas, etc)
- Copias de seguridad (Fallos en elementos de copias, fallos en soportes cintas, discos, robot, etc)
- Información (Bases de datos, ficheros, manuales, procedimientos, planes de contingencia, etc)
- Personal (Errores y ataques de personal interno, externo, funciones, perfiles, formación, etc)
- Riesgos contra el patrimonio (Robo, pérdida no intencionada de activos, etc)
- Otros riesgos (Terrorismo, epidemias, confianza de los clientes, imagen de empresa, insolvencia de servicios externos, seguros, outsourcing, etc)

1.2 Objetivos

1.2.1 Objetivo general

Reducir y mitigar los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnología de Card Perú S.A. que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos. (Ver Anexo 2)

1.2.2 Objetivos específicos

- Implementar una Política de Seguridad de Información que sea desplegada a todos los colaboradores, proveedores y terceros involucrados en los procesos de tecnología.
- Gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de la información, para reducirlos en un 80%.
- Desplegar las medidas de seguridad para gestionar los riesgos y ejecutar controles de tratamiento de riesgos, para reducir el 90% de los riesgos a niveles aceptables
- Formación y concientización al 100% de los colaboradores involucrados en los procesos de Tecnología, en temas de seguridad de información.
- Cumplimiento de la legislación vigente sobre información personal, propiedad intelectual y otras.
- Gestionar y controlar el 100% de los documentos del SGSI.

1.3 Justificación

Debido a los riesgos a los que están expuestos los activos de información, el impacto que la interrupción de estos puede causar, es preponderante la definición de una metodología y el uso de herramientas que nos ayuden reducir y mitigar estos riesgos.

Es por ello que se propone la implementación de un Sistema de gestión de seguridad de información (SGSI), el cual nos brindará los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información, implantar los controles necesarios que ayudarán a salvaguardar los activos de información de los procesos de tecnología, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de Información (SGSI), alineándolo de esta manera a los objetivos estratégicos de la organización. (Selección de la Metodología Ver Anexo 3)

1.4 Limitaciones

El proyecto se ejecutará en la empresa Card Perú S.A. donde se realizará el diseño y la implementación de un Sistema de gestión de seguridad de información (SGSI) enfocado a los “Procesos de tecnología”.

1.4.1 Alcance del proyecto: mapa de procesos de tecnología - Card Perú S.A.

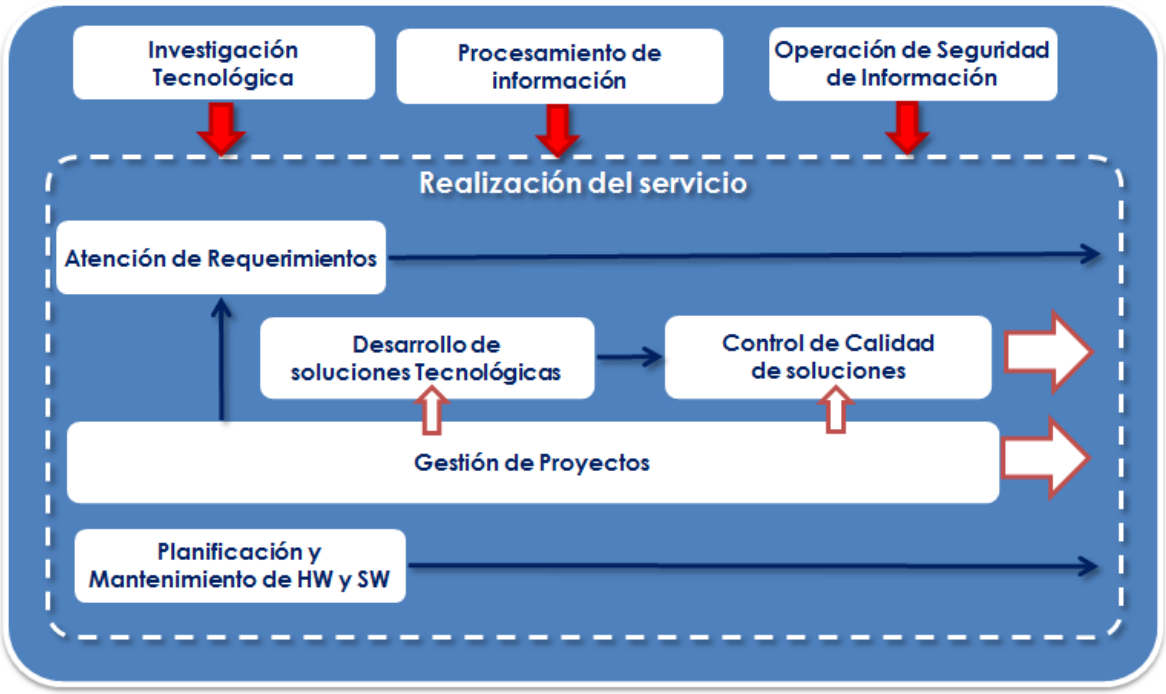


Gráfico 1.1: Mapa de procesos Card Perú S.A [1]

1.4.2 Procesos de tecnología

Los procesos de tecnología de la organización dentro del alcance del SGSI son los siguientes:

- **(1)** Gestión de proyectos
- **(2)** Desarrollo de soluciones tecnológicas
- **(3)** Control de calidad de soluciones
- **(4)** Atención de requerimientos
- **(5)** Procesamiento de información
- **(6)** Planificación del mantenimiento de hardware y software

[1] Elaboración: los autores.

- **(7)** Investigación tecnológica
- **(8)** Operación de seguridad de información

1.4.3 Limitaciones del proyecto

Para el desarrollo del proyecto se presentaron las siguientes limitaciones:

- ✓ Capacidad del personal por carga laboral,
- ✓ Disposiciones presupuestarias,
- ✓ Acotadas fechas de entrega,
- ✓ Aprobaciones de organismos gerenciales

1.4.4 Mitigación de limitaciones del proyecto:

Limitación	Plan de acción
Capacidad del Personal por carga laboral	✓ Terciarizar personal para la realización de las actividades
Disposiciones presupuestarias	✓ Priorización de nuevos recursos informáticos, ✓ Alianzas estratégicas con proveedores para compras a largo plazo, ✓ Mantener recursos informáticos usados (Ampliar garantía)
Acotada fechas de entrega	✓ Incrementar horas hombre en la implementación del Proyecto
Aprobaciones de organismos gerenciales	✓ Identificar decisiones y documentos críticos ✓ Diferenciar decisiones y documentos que requieren alto nivel de responsabilidad. ✓ Segregar responsabilidades para aprobaciones.

Cuadro 1.1: Mitigación de limitaciones del proyecto [2]

[2] Elaboración: los autores.

1.5 Viabilidad

1.5.1 Viabilidad técnica

Es técnicamente posible la implementación del sistema de gestión de seguridad de información por los siguientes motivos:

- ✓ El hardware a utilizar es compatible con la infraestructura actual de la organización, por lo que no se tendría problema para la implantación del proyecto.
- ✓ El software a utilizar, en su mayoría, serán propios de la organización; solo se adquirirán nuevas licencias y actualizaciones, por lo que no se tendría problemas para la implantación del proyecto.
- ✓ El sistema core de la organización, el as/400, es un equipo de IBM de gama alta para todo tipo de empresas grandes.
- ✓ Todo el personal está capacitado con la infraestructura actual de la organización. las nuevas tecnologías que se adquirirán serán previamente capacitadas por el proveedor, por lo que no se tendría problemas para la implementación del proyecto.

1.5.2 Viabilidad económica

Es económicamente posible, ya que el ahorro supuesto anual que se obtiene tras la implementación del SGSI es de 1 450 000 nuevos soles, los ingresos de Card Perú S.A. en el 2011 fueron de 400 000 000, y el costo de implementación del proyecto es 339 820. Para conocer con más detalle los datos indicados ver 3.2.1.2.5 (Análisis costo/beneficio).

1.5.3 Viabilidad social

- **Beneficios a la sociedad**

  No aplica

- **Impacto en el medio ambiente**

  Para la implementación de un SGSI, es necesario consumir diversos recursos adicionales que impactan en el medio ambiente, siendo estos:

✓ Generación de papeles

✓ Generación de residuos peligrosos: (tóner de impresoras, cintas de impresión de máquinas de escribir, etc.)

✓ Consumo de energía (luces generales e informática)

- **Conclusión**

  La organización actualmente viene consumiendo estos recursos que impactan ambientalmente; con la Implementación del SGSI, el impacto será aún mayor. Para ello se elaboran las b**uenas prácticas ambientales** (**Ver anexo 04**)

1.5.4 Viabilidad operativa

- **Posibles restricciones a la puesta en marcha del proyecto**
  - ✓ Gerencia reduce el tiempo de implementación del SGSI.
  - ✓ Gerencia no aprueba el costo de la implementación del SGSI.
  - ✓ Gerencia amplia el alcance del SGSI.
  - ✓ Recursos necesarios no disponibles para la implementación.
- **Los requisitos de mercado**
  - ✓ Aceptación de depósitos y otros fondos rembolsables del público.
  - ✓ Préstamo de todo tipo.
  - ✓ Servicios de arrendamiento financiero.
  - ✓ Todos los servicios de pago y transferencia monetaria.
  - ✓ Garantías y compromisos.

- ✓ Servicios de pago y compensación respecto de otros activos financieros.
- ✓ Participación en emisiones de toda clase de valores.
- ✓ Servicios de pago y compensación respecto de otros activos financieros.
- ✓ Intercambio comercial por cuenta propia o de clientes, ya sea en una bolsa, en un mercado extrabursátil o de otro modo de:
    - Instrumentos del mercado monetario como son: cheques, letras, certificados de depósitos, etc.
    - Moneda extranjera.
    - Instrumentos de los mercados cambiario y monetario, por ejemplo, “swaps” y acuerdos a plazo sobre tipos de interés.
    - Valores negociables.
    - Otros instrumentos y activos financieros negociables.
- ✓ Servicios de asesoramiento y los demás servicios financieros auxiliares.

- **Ampliaciones futuras**

  Card Perú S.A. busca convertirse en una entidad financiera para mediados del 2012. Para ello es necesario que cumpla con una serie de requisitos exigidos por la Superintendencia de Banca y Seguros (SBS), siendo uno de los más importantes contar con Sistema de Gestión de Seguridad de Información.

- **Conclusión**

  Se concluye de los puntos mencionados anteriormente, que implementando un Sistema de Gestión de Seguridad de Información basado en la ISO 27001:2005, Card Perú acortará la brecha con la que actualmente cuenta respecto a las entidades financieras, pudiendo en el futuro ofrecer los servicios requeridos por el mercado financiero.

CAPÍTULO II
MARCO TEÓRICO

Los conceptos que se utilizan para la elaboración de la tesis son los siguientes.

2.1 Sistema de gestión de seguridad de la información (SGSI)

Un Sistema de Gestión de Seguridad de Información es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa (ISO 17799:2005; Alexander, 2007). Un SGSI está soportado en cuatro grandes y continuas etapas para su mantención en el tiempo, las cuales son:

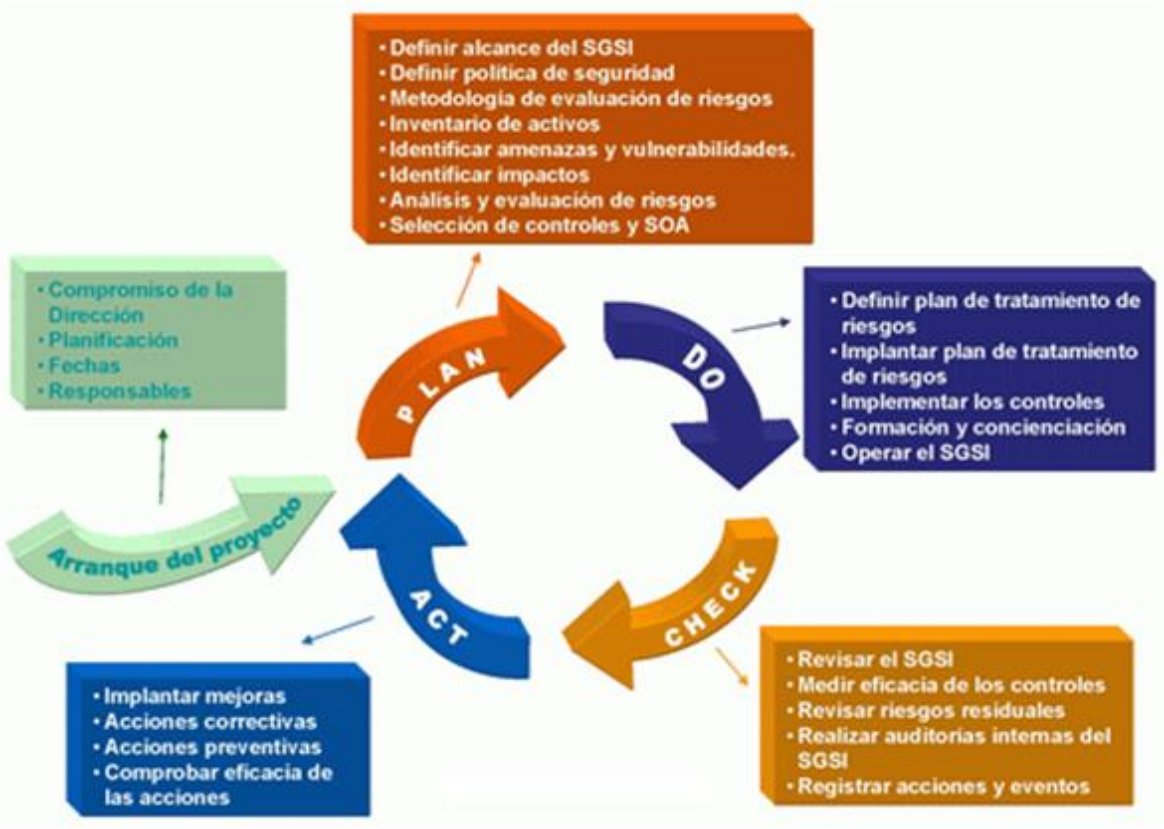


Gráfico 1.2: Etapas de SGSI [3]

2.1.1 Seguridad de información

"Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma". [4]

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos saber que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc. La información es poder, y según las posibilidades estratégicas que ofrece tener a acceso a cierta información, ésta se clasifica como:

- **Crítica**: Es indispensable para la operación de la empresa.
- **Valiosa**: Es un activo de la empresa y muy valioso.
- **Sensible**: Debe ser conocida por las personas autorizadas

Los términos de seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información.

2.1.2 Activo de información

Según Alexander (2007, 44) "Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones. Para cualquier tipo de empresa son de vital importancia la gestión y la responsabilidad por los activos.

En este punto es importante clarificar que es un activo de información. Según el ISO 17799:2005 (Código de práctica para la gestión de seguridad de información), un activo de información es algo a lo que una organización directamente le asigna

3 Fuente: El Gráfico se obtuvo del portal de la ISO en español ubicado en el siguiente enlace: http://www.iso27000.es/sgsi.html

4 Fuente: Definición que se tomó como referencia del siguiente enlace: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

un valor y, por lo tanto, la organización debe proteger. Los activos de información se pueden clasificar en las siguientes categorías:

- Activos de información (datos, manuales de usuario, etc.).
- Documentos de papel (contratos).
- Activos de software (aplicación, software de sistemas, etc.).
- Activos físicos (computadoras, medios magnéticos, etc.).
- Personal (clientes, empleados).
- Imagen de la compañía y reputación
- Servicios (comunicaciones, etc.).”

2.1.3 Confidencialidad

La confidencialidad es la propiedad para prevenir la divulgación de información a personas o sistemas no autorizados. Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad. [5]

2.1.4 Integridad

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que

[5] Fuente: Definición tomada del siguiente enlace:
http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

son parte de la información, asimismo, hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información. [6]

2.1.5 Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad en sistemas tiene como objetivo estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

La disponibilidad además de ser importante en el proceso de seguridad de la información es, además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web, etc; mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar. [7]

2.1.6 Vulnerabilidad

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

---

[6] Fuente: Definición que hace referencia al concepto de disponible y fue extraída del siguiente enlace: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

[7] Fuente: Definición disponibilidad extraída de la enciclopedia virtual Wikipedia y se encuentra en el siguiente enlace: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza afecte un activo.

Las vulnerabilidades pueden clasificarse como:

- Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimientos que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).
- Control de acceso (segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para el control de acceso, passwords sin modificarse).
- Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, susceptibilidad de equipos a variaciones de voltaje).
- Gestión de operaciones y comunicaciones (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión).
- Mantenimiento, desarrollo y adquisición de sistemas de información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software,

documentación pobre de software, mala selección de ensayo de datos).

Cabe destacar que las vulnerabilidades y las amenazas deben presentarse juntas para poder causar incidentes que pudiesen dañar los activos. Por esta razón es necesario entender la relación entre amenazas y vulnerabilidades. La pregunta fundamental es: ¿Qué amenaza pudiese explotar a cuál de las vulnerabilidades? (Alexander, 2007)

2.1.7 Amenaza

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado, que puede generar daño a la organización y a sus activos.

Una amenaza es la indicación de un potencial evento no deseado. Esta definición hace referencia a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural.

Para una empresa, las amenazas pueden ser de distintos tipos con base en su origen. Las amenazas se pueden clasificar en:

- Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, pérdida de acceso, fallas mecánicas).
- Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- Amenazas operacionales (crisis financiera, pérdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad).
- Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

Como se nota las amenazas se pueden generar de fuentes o eventos accidentales o deliberados.

Para que una amenaza cause daño a un activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en su intención de hacer daño. (Alexander, 2007)

2.1.8 Definición del riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

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

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de causalidad y probabilidad de ocurrencia.

Gráfico 1.3: Elementos del riesgo [8]

[8] Fuente: Gráfico que muestra la interrelación entre los elementos del riesgos, fue extraído del siguiente enlace: http://cata-seguridaddelainformacion.blogspot.com/

2.1.9 Riesgo residual

Es el riesgo remanente después de haber realizado el tratamiento del riesgo.

2.1.10 Control

Aquellos mecanismos y/o procedimientos que regulan el propio funcionamiento del SGSI.

2.1.11 International Organization for Standardization (ISO)

La Organización Internacional de Normalización o ISO nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

La ISO es una red de los institutos de normas nacionales de 162 países, sobre la base de un miembro por país, con una Secretaría Central en Ginebra (Suiza) que coordina el sistema. La Organización Internacional de Normalización (ISO), con sede en Ginebra, está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento ambiental.

Las normas desarrolladas por ISO son voluntarias, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país. El contenido de los estándares está protegido por derechos de copyright y para acceder a ellos el público corriente debe comprar cada documento, que se valoran en francos suizos (CHF). [9]

[9] Fuente: Definición de la norma ISO extraída del siguiente enlace: http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_de_Normalizaci%C3%B3n

2.1.12 International Electrotechnical Commission (IEC)

La Comisión Electrotécnica Internacional es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas. Numerosas normas se desarrollan conjuntamente con la ISO (normas ISO/IEC).

La IEC, fundada en 1904 durante el Congreso Eléctrico Internacional de San Luis (EEUU), y cuyo primer presidente fue Lord Kelvin, tenía su sede en Londres hasta que en 1948 se trasladó a Ginebra. Integrada por los organismos nacionales de normalización, en las áreas indicadas, de los países miembros, en 2003 pertenecían a la IEC más de 60 países.

En 1938, el organismo publicó el primer diccionario electrotécnico internacional (International Electrotechnical Vocabulary) con el propósito de unificar la terminología eléctrica, esfuerzo que se ha mantenido durante el transcurso del tiempo, siendo el Vocabulario Electrotécnico Internacional un importante referente para las empresas del sector. [10]

2.1.13 ISO/IEC 27001:2005

La ISO 27001:2005 está orientada a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las empresas, de amenazas externas o internas.

Es importante entender que la ISO/IEC 27001:2005 se ha desarrollado como modelo para el establecimiento, la implementación, la operación, el monitoreo, la revisión, el mantenimiento y la mejora de un SGSI para cualquier clase de organización.

2.1.14 ISO/IEC 27002:2005

"Código de prácticas para la gestión de la seguridad de la información". Es un modelo que da recomendaciones para las buenas prácticas. Es un modelo basado en el anexo A de la ISO/IEC 27001:2005, el cual amplía y explica de forma detalla cómo implantar los controles del anexo A de la ISO/IEC 27001:2005 Este método no puede utilizarse para la certificación. (Alexander, 2007)

[10] Fuente: definición de la organización IEC extraída del siguiente enlace: http://es.wikipedia.org/wiki/Comisi%C3%B3n_Electrot%C3%A9cnica_Internacional

2.1.15 Política de seguridad

Son las directrices y objetivos generales de una empresa relativos a la seguridad, expresados formalmente por la dirección general. La política de seguridad forma parte de la política general y debe ser aprobada por la alta dirección.

La Política de seguridad de una empresa es un documento auditable ya sea por los auditores internos de la empresa o por externos en busca de una certificación, inclusive por el cliente. Por este motivo este documento debe ser entendido a todos los niveles, desde el personal operativo / operador hasta los altos mandos (directores, gerentes, etc.).

Una política de seguridad es como la "carta de presentación de la empresa" donde se exponen los puntos que quiere dar a conocer la empresa, ¿a qué se dedica?, ¿qué quiere lograr?, ¿bajo qué método trabaja?, ¿Cómo lo quiere lograr? Estas cuatro preguntas son la estructura que debe llevar la carta de presentación ante el cliente, el quien al leer estos cuatro puntos va a tener una idea muy clara de la empresa a la que está a punto de comprar sus productos o servicios.

Existen cuatro pasos esenciales para lograr un fácil entendimiento y estructuración de una política de seguridad.

- *¿A qué se dedica?* Como primer punto, se requiere una clara explicación del giro y dedicación de la empresa. Esto es muy esencial aunque parezca que no. Por ejemplo: En la empresa "Hules Internacionales" nos dedicamos a la elaboración de hules mediante la aplicación de estrictas normas de control y trazabilidad de nuestro producto.
- *Credibilidad y confianza en el mercado (¿Qué quiere lograr?)*La credibilidad y confianza de los distintos actores que intervienen en las operaciones de comercio. La seguridad y control en todos sus procesos incrementa la confianza en sus operaciones y por ende una ampliación de los beneficios de la empresa recibiendo mejor trato y aceptación. Por ejemplo: manteniendo prácticas seguras en todos los procesos para que nuestra empresa no sea utilizada por

individuos u organizaciones que quieren cometer actos ilícitos, garantizando la transparencia y legalidad de nuestras operaciones y por ende mayor satisfacción e imagen de nuestro producto o servicio.

- *Norma de aplicación (¿Bajo qué método trabajo?)*Se recomienda mencionar la norma de aplicación que esté usando la empresa para promocionar sus logros y métodos de trabajo. Por ejemplo: Mediante la implementación de estándares internacionales de seguridad.
- *Mejora continua*: Es importante mencionar que se trabaja mediante un proceso denominado mejora continua, esta es crecer y mejorar pero de forma imparable, el estancamiento no permite nunca la mejora continua. Por ejemplo: Alcanzando la mejora continua en todos los procesos de la organización. [11]

2.2 Entidad financiera

"Una entidad financiera es cualquier empresa que presta servicios financieros (captación y remuneración de nuestros ahorros, concesión de préstamos y créditos, aseguramiento, etc.) a los consumidores y usuarios.

Para la normativa de protección del consumidor, las entidades financieras abarcan a tres tipos de empresas que prestan servicios a sus usuarios:

- Las entidades de crédito (bancos, cajas de ahorro, etc.),
- Las empresas de servicios de inversión, y
- Las entidades aseguradoras.

Estas empresas están sometidas a un control administrativo por entidades regulatorias, como la Superintendencia de Banca, Seguros y AFP (**SBS**), teniendo una serie de obligaciones de seguridad de información, solvencia y transparencia." [12]

[11] Fuente: Definición de política de seguridad parafraseada de la información ubicada en el siguiente link http://www.basc-costarica.com

[12] Fuente: Definición de entidad financiera que fue extraída del siguiente enlace: http://www.consumoteca.com/economia-familiar/economia-y-finanzas/entidades-financieras

2.3 Circular n° g-140

Es una circular de cumplimiento obligatorio, que establece requisitos mínimos de cumplimiento respecto a la Gestión de la Seguridad de Información, y es de aplicación a empresas del sector financiero, tales como: cajas municipales de Ahorros, bancos, entidades financieras, entre otras. (Ver Anexo 01).

2.4 Departamentos de gerencia de tecnología

Los departamentos de la gerencia de tecnología son: business intelligence, desarrollo y centro de cómputo. Estos departamentos se describen a continuación:

2.4.1 Departamento de Business Intelligence

Departamento encargado del análisis, explotación y enriquecimiento de información valiosa para la organización.

2.4.2 Departamento de Desarrollo

Departamento encargado de los desarrollos de software en las diferentes plataformas de desarrollo. (AS/400, .Net, Visual Basic y Java)

2.4.3 Departamento de Centro de Cómputo

Departamento encargado de brindar toda infraestructura tecnológica adecuada para la operatividad de toda la organización.

2.5 Metodología de gestión de riesgos (alexander, 2007) [13]

La metodología de gestión de riesgos mostrada a continuación es una recopilación de buenas practicas para el análisis y evaluación de riesgos extraída del libre de Alexander, 2007.

2.5.1 Identificación de activos

Los activos de información en la empresa, dentro del alcance del SGSI, son fundamentales para una correcta implementación de un SGSI.

El análisis y la evaluación del riesgo y las decisiones que se tomen en relación con el tratamiento del riesgo en la empresa giran alrededor de los activos de información identificados.

[13] Fuente: Metodología de gestión de riesgos extraída de “Diseño de un sistema de gestión de seguridad de información” de Alberto Alexander.

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, necesitan tener protección para asegurar una correcta operación del negocio y continuidad en sus operaciones. Para cualquier tipo de empresa son de vital importancia la gestión y la responsabilidad por los activos.

En este punto es importante clasificar los activos de información. Estos se clasifican en las siguientes categorías:

- ✓ Activos de información (datos, manuales de usuario, etc.)
- ✓ Documentos de papel (contratos)
- ✓ Activos de software (aplicación, software de sistemas, etc.)
- ✓ Activos físicos (computadoras, medios magnéticos, etc.)
- ✓ Imagen de la compañía y reputación
- ✓ Servicios (comunicaciones, etc.)

Como se aprecia, los activos de información son muy amplios. Es fundamental estar conceptualmente claros de qué es un activo de información y conocer sus distintas posibles modalidades, para así poder realizar un correcto análisis y una evaluación y, por ende, poder establecer adecuadamente el modelo ISO 27001:2005.

La metodología de las elipses (ver 3.1.3.2.4 B) desempeña un papel muy importante en esta etapa. Con base en las elipses, la empresa, considerando la categorización de los activos, debe iniciar la identificación de los activos de información.

En la organización, el proceso de identificación y tasación de activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en los procesos y subprocesos que abarca el alcance del modelo. Es muy importante que los dueños de los activos principales conformen el grupo multidisciplinario. Como un “dueño de activos” se entiende aquella persona que tiene una responsabilidad por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos, aprobada por la gerencia. Dentro del alcance del SGSI, los activos importantes deben identificarse con

claridad, como ya se explicó, y posteriormente deben ser tasados para visualizar su impacto en la empresa por su deterioro o por sus fallas en: (1) confidencialidad, (2) integridad y (3) disponibilidad.

2.5.2 Identificación de requerimientos legales y comerciales relevantes para los activos identificados

- ✓ La primera fuente deriva de la evaluación de los riesgos que afectan a la organización. Aquí se determinan las amenazas de los activos, luego se ubican las vulnerabilidades, se evalúa su posibilidad de ocurrencia y se estiman los potenciales impactos.
- ✓ La segunda fuente es el aspecto legal. Aquí están los requerimientos contractuales que deben cumplirse.
- ✓ La tercera fuente es el conjunto particular de principios, objetivos y requerimientos para procesar información que la empresa ha desarrollado para apoyar sus operaciones.

Al identificar los activos de información, se deben analizar si existen requerimientos legales y comerciales relacionados con los activos identificados. Si hubiera requerimientos legales o comerciales, se debe revisar si dichos requerimientos involucran otros activos de información.

2.5.3 Tasación de activos

Cada activo se tasa, utilizando una escala de Likert. El valor 1 significa “muy poco” y 5 “muy alto”. La pregunta que debe efectuarse para utilizar la escala es: ¿Cómo una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?

El propietario de los activos debe ser responsable de definir apropiadamente la clasificación de seguridad y los derechos de acceso a los activos. La responsabilidad del propietario debiera ser también la de revisar periódicamente los derechos de acceso y la clasificación de seguridad. Además de esto, debiera ser útil definir, documentar e implementar reglas para el uso aceptable de activos, describiendo acciones permitidas y prohibidas en el uso cotidiano de los activos. Las personas que utilizan los activos, deben estar conscientes de estas reglas como parte de su descripción del puesto.

2.5.4 Identificación de amenazas y vulnerabilidades

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus activos.

"Una amenaza es la identificación de un potencial evento no deseado". En esta definición, los autores se refieren a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural. En su libro *Information Segurity Risk Analysis (*Welter, 2001*),* Thomas Welter plantea que una amenaza puede significar muchas cosas, depende del contexto en donde se le ubique.

- ✓ Clasificación de amenazas

Cuando la empresa inicia la identificación de amenazas que pudiesen afectar sus activos, conviene clasificarlas por su naturaleza, para así facilitar su ubicación. Las categorías de las amenazas difieren en los papeles relativos que los seres humanos y los factores aleatorios desempeñan en relación con su causalidad. En consecuencia, también difieren los métodos para estimar su posibilidad de ocurrencia:

- Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, pérdida de acceso, fallas mecánicas).
- Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- Amenazas operacionales (crisis financiera, pérdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad).
- Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

- ✓ Vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza afecte un activo. Las vulnerabilidades pueden clasificarse como:

- Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimientos que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).
- Control de acceso (segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para el control de acceso, passwords sin modificarse).
- Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, susceptibilidad de equipos a variaciones de voltaje).
- Gestión de operaciones y comunicaciones (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión).
- Mantenimiento, desarrollo y adquisición de sistemas de información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de

validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayo de datos).

Una vez identificadas las vulnerabilidades, por cada una de ellas, se debe evaluar la posibilidad de que sean explotadas por la amenaza.
Es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos.

- ✓ Revisión de controles implementados

En algún momento previo al inicio de las actividades del cálculo del riesgo, o antes de identificar las amenazas y vulnerabilidades, deben identificarse los controles ya existentes en el sistema para medir su eficacia. Un control ineficaz es una vulnerabilidad.

2.5.5 Cálculo de las amenazas y vulnerabilidades

Una vez identificadas las amenazas y vulnerabilidades, es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo. El riesgo se define como “la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular” (Peltier, 2001). Todo este proceso incluye calcular la posibilidad de que la ocurrencia de amenazas y que tan fácil pueden ser explotadas las vulnerabilidades por las amenazas. Conviene calcular la posibilidad de la presencia de amenazas; para este fin se deben considerar los siguientes aspectos de las amenazas:

- ✓ Amenazas deliberadas. La posibilidad de amenazas deliberadas en la motivación, conocimiento, capacidad y recursos disponibles para posibles atacantes y la atracción de los activos para sofisticados atacantes.
- ✓ Amenazas accidentales. La posibilidad de amenazas accidentales puede estimarse utilizando la experiencia y las estadísticas.
- ✓ Incidentes del pasado. Los incidentes ocurridos en el pasado ilustran los problemas en el actual sistema de protección.
- ✓ Nuevos desarrollos y tendencias. Esto incluye informes, novedades y tendencias obtenidas de diferentes medios, como Internet.

2.5.6 Análisis del riesgo y su evaluación

El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

La organización debe decidir el método para hacer el cálculo del riesgo que sea más apropiado para la empresa y los requerimientos de seguridad. Los niveles de riesgo calculados proveen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.

2.6 Metodología de análisis y gestión de riesgos de los sistemas de informacion (magerit) [14]

Es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información. A continuación, se procede a explicar la metodología.

1 Objetivos del Magerit

Magerit persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

[14] Fuente: Definición de Magerit extraída del siguiente enlace: https://www.ccn-cert.cni.es/publico/herramientas/pilar43/magerit/meth-es-v11.pdf

2 Enfoque y gestión de riesgos en Magerit

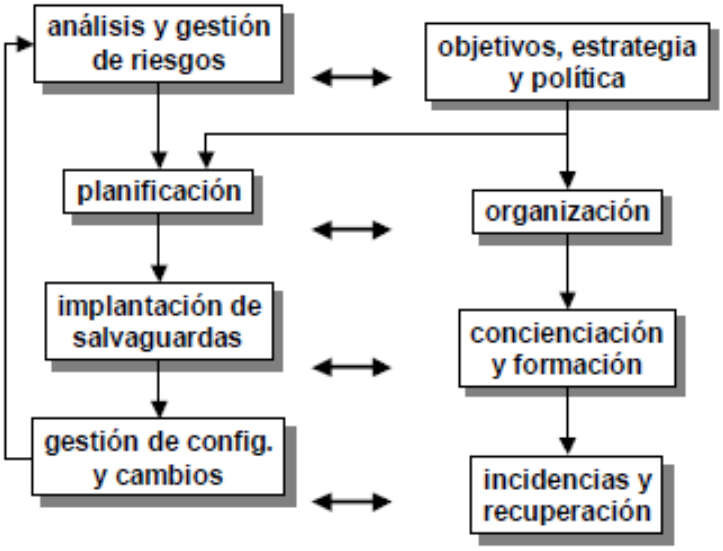
Las tareas de análisis y gestión de riesgos no son un fin en sí mismas sino que se encajan en la actividad continúa de gestión de la seguridad.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta la Dirección.

La implantación de los controles de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

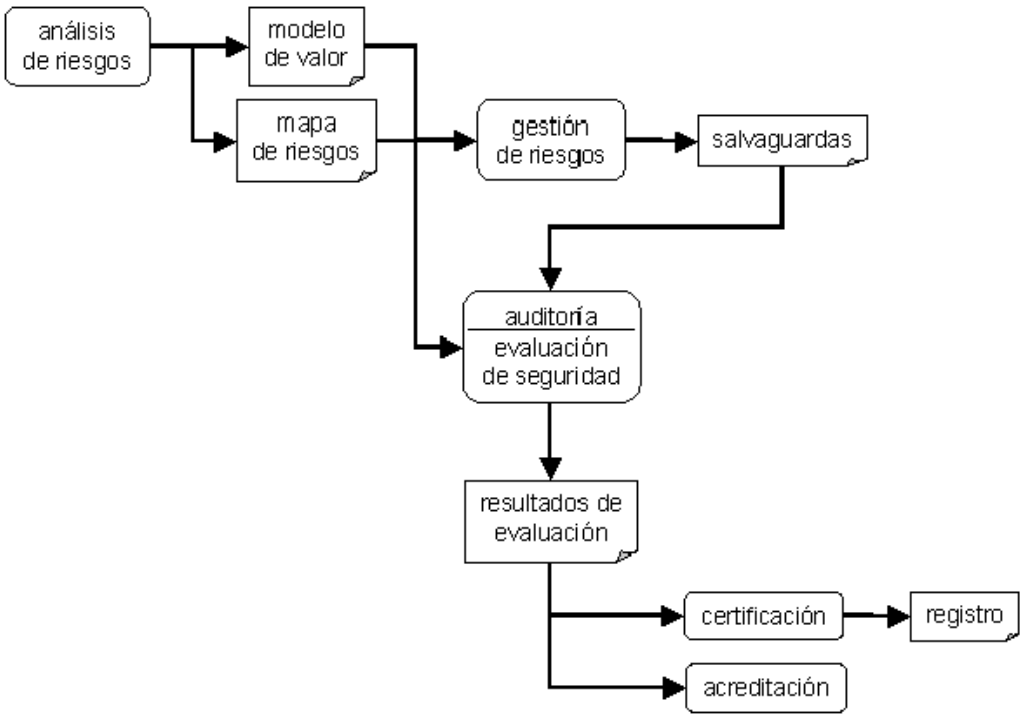
El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.



(Fuente: Magerit, Pág.8)

3 Evaluación, certificación, auditoria y acreditación

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. En análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué salvaguardas se ha dotado. Es pues el análisis de riesgos paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema:



(Fuente: Magerit, Pág.12)

4 Realización del análisis y de la gestión del riesgo

a. Análisis de riesgos, permite determinar qué tiene la Organización y estimar lo que podría pasar. Elementos:

- ✓ activos, que no son sino los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la Organización
- ✓ amenazas, que no son sino cosas que les pueden pasar a los activos causando un perjuicio a la Organización
- ✓ salvaguardas (o contra medidas), que no son sino elementos de defensa desplegados para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

- ✓ el impacto: lo que podría pasar
- ✓ el riesgo: lo que probablemente pase

b. Gestión de riesgos, permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los

incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume. Si el impacto y el riesgo residuales son despreciables, se ha terminado. Si no, hay que hacer algo

- ✓ **Interpretación de los valores de impacto y riesgo residuales**

  Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores despreciables. Son pues una métrica de carencias.

  Los párrafos siguientes se refieren conjuntamente a impacto y riesgo.

  Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

  Si el valor residual es despreciable, ya está. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza

- ✓ **Selección de salvaguardas**

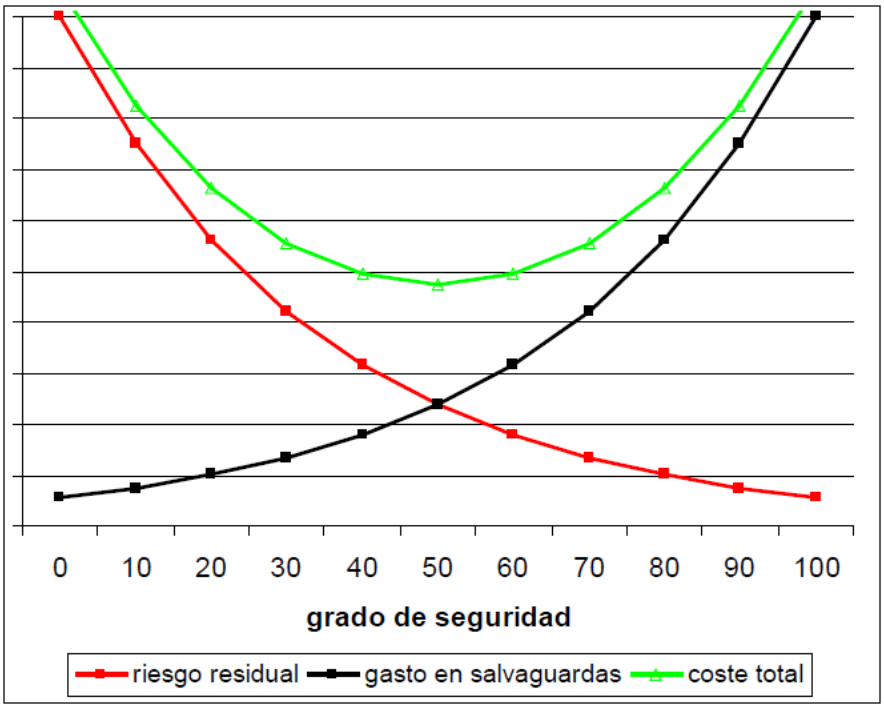
  Las amenazas hay que conjurarlas, por principio y mientras no se justifique lo contrario.

  Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades)

- ✓ **Pérdidas y ganancias**

  Es de sentido común que no se puede invertir en salvaguardas más allá del valor de los propios activos a proteger.

  Aparecen en la práctica gráficos como el siguiente que ponen uno frente al otro el coste de la inseguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas



(Fuente: Magerit, Pág.28)

- ✓ **Cambio de actitud de la dirección**

  La dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias.

  Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, etc)

5 Desarrollo de un proyecto Magerit

a. Planificación

- ✓ Se establecen las consideraciones necesarias para arrancar el proyecto.
- ✓ Se investiga la oportunidad de realizarlo.
- ✓ Se definen los objetivos que ha de cumplir y el dominio (ámbito) que abarcará.
- ✓ Se planifican los medios materiales y humanos para su realización.

- ✓ Se procede al lanzamiento del proyecto.

b. Análisis de riesgos

- ✓ Se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen.
- ✓ Se identifican las amenazas significativas sobre aquellos activos y se valoran en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.
- ✓ Se identifican las salvaguardas existentes y se valora la eficacia de su implantación.
- ✓ Se estima el impacto y el riesgo al que están expuestos los activos del sistema.
- ✓ Se interpreta el significado del impacto y el riesgo.

c. Gestión de riesgos

- ✓ Se elige una estrategia para mitigar impacto y riesgo.
- ✓ Se determinan las salvaguardas oportunas para el objetivo anterior.
- ✓ Se determina la calidad necesaria para dichas salvaguardas.
- ✓ Se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- ✓ Se lleva a cabo el plan de seguridad.

2.7 Entorno del mercado

A continuación se presenta una breve descripción del inicio de las entidades financieras.

A comienzos del siglo pasado, aparecieron nuevas formas de pago, una de ellas es la tarjeta de crédito que se ha desarrollado y difundido agigantadamente.

Las tarjetas de crédito son un medio de pago futuro que debe de ser pagado en un tiempo determinado hacia una entidad financiera, por el cual se evalúan de manera distinta y determinada a todo tipo de clientes ya que las características o los ingresos mensuales de cada uno son diferentes a los de otro, por el lado de las entidades financieras algunas de estas se toman la libertad de poder escoger a estos tipos de clientes, es decir usan bases de datos internas con la información

detallada de cada uno de estos para poder así, brindarles el mejor servicio acorde a sus necesidades.

Las tarjetas de crédito pueden ser emitidas solamente por empresas bancarias, financieras y empresas del sistema financiero, o algunas que puedan o tengan la facultad de emitir tarjetas de crédito (Card Perú S.A.), según la ley N° 26702. La línea de crédito otorgada es calculada en función de la documentación presentada por el titular, la misma es muy importante ya que de los ingresos y egresos depende la línea de crédito a asignar.

La crisis financiera no pudo con ellas y pese a que han sido satanizadas, debido a las altas tasas de interés que cobran los bancos, las tarjetas de crédito siguen siendo uno de los medios de pago favorito de los peruanos.

“La mejora en la situación económica ha contribuido a que el nivel de ocupación crezca, posibilitando que más peruanos tengan ingresos estables y se conviertan en tarjetahabientes”, explica Rolando Castellares, experto en temas bancarios.

La mayor competencia generada por la apertura de nuevas entidades financieras llevó a que los bancos empezaran a ‘bancarizar’ (incorporar al sistema) a quienes antes no eran considerados sujetos de créditos, como los trabajadores independientes o los microempresarios informales.

Las entidades financieras frecuentemente están amenazadas por riesgos que ponen en peligro la integridad de la información, procesos y con ello la viabilidad del negocio. Riesgos que provienen no solo desde el exterior como mafias, hackers, crackers, sino también desde el interior como empleados, sucursales, proveedores. Las entidades financieras pueden asegurar sus datos e información con la ayuda de un sistema de gestión de seguridad de la información (SGSI).

Un SGSI ofrece la posibilidad de disponer de controles que mitigan los riesgos a los que se someten los activos. Estas acciones van a proteger a la entidad financiera frente a amenazas y riesgos que puedan poner en peligro los datos de

clientes y la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzas los objetivos de negocio financiero.

2.8 Antecedentes

Un estudio realizado por el diario La República (2011), indica que el 15% de las firmas encuestadas sufrieron por acceso a información confidencial por parte de sus empleados, el14% por intrusión de personas ajenas, al 42% les robaron sus computadores portátiles y el 6% perdió sus teléfonos móviles. Desprendiéndose de lo antes mencionado, las pérdidas financieras ocasionadas por delitos informáticos ascendieron a $200.000 el año anterior, según el Computer Crime and Security Survey (CSI). A continuación se presenta un ejemplo de antecedente nacional y otro internacional de implementación de un SGSI.

2.8.1 Antecedente nacional

Como un claro ejemplo de la implementación de un SGSI en Perú basado en la norma ISO/IEC 27001:2005 tenemos a la empresa Telefónica del Perú.

Telefónica del Perú alcanzó con éxito la Certificación Internacional ISO/IEC 27001:2005, para su data center donde brinda servicios de outsourcing de TI, disaster recovery / business continuity, hosting, a las empresas de mayor envergadura en el país, así como para sus centros de gestión de móviles, de banda ancha y de redes empresariales, elevándose a estándares de clase mundial.

De esta manera, la gestión de las direcciones de outsourcing y data center y de gestión de red, han sido reconocidas por la adecuada implementación y operación de sus sistemas de gestión de seguridad de la información (SGSI).
Esta certificación es un gran hito para Telefónica del Perú, pues la posiciona como la operadora de Latinoamérica con la certificación ISO 27001 de mayor alcance y la única que cuenta con la gestión de los servicios móviles y de gestión del data center certificada. Así, Telefónica demuestra su compromiso con el cliente basado en la mejora continua, garantizando niveles de servicio que

permitan obtener información cuando la organización lo necesite; es decir, disponible las 24 horas, siete días a la semana, los 365 días del año.

Esto permite que en adelante se pueda incorporar a la oferta de Telefónica una credencial que los diferencia no solo en Perú, sino también en Latinoamérica, dentro y fuera del Grupo Telefónica ya que cuenta con un sistema de gestión de la seguridad de la información certificado bajo una norma internacional tanto para las redes como para los servicios de TI. Además, implica una gran ventaja competitiva ya que la preservación de la información crítica de sus clientes empresariales es una exigencia del mercado al integrarse cada vez con mayor intensidad redes y sistemas, generándose un valor agregado extremo a extremo para sus servicios.

Esta certificación, otorgada por AENOR Internacional, es un estándar internacional con un alto grado de tecnicidad y rigurosidad, por lo cual sólo las principales organizaciones del mundo logran obtenerla (operadoras de telecomunicaciones, fabricantes de tecnología, organismos de seguridad e instituciones financieras).

De ahí que es necesario recalcar que seguridad de la información es mucho más que implementar “firewalls”, aplicar parches para corregir nuevas vulnerabilidades en el sistema de software, protegerse de amenazas externas o guardar en la bóveda los “backups”. Seguridad de la Información es determinar qué requiere ser protegido, por qué, de qué y cómo; todo esto bajo un modelo integral de gestión.

Este reconocimiento confirma la implantación exitosa de los elementos de seguridad que garantizan la confidencialidad, integridad y disponibilidad de la información de los clientes de Telefónica y reconoce el éxito de los procedimientos que aplica la empresa para resolver eficazmente las incidencias de seguridad de sus usuarios, reduciendo la afectación de sus servicios.

Este logro alcanzado posiciona a Telefónica del Perú como la operadora líder del Grupo Telefónica Latinoamérica en alcanzar este objetivo y promover la gestión de la seguridad de las redes y plataformas. Todo esto gracias

a la solidez de los sistemas implementados y el buen trabajo realizado por todas sus áreas implicadas. [15]

2.8.2 Antecedente internacional

Bankinter es la primera entidad financiera española en obtener esta certificación para sus plataformas y sistemas informáticos.

Bankinter ha recibido de British Standard Institution (BSI) la certificación internacional ISO/IEC 27001:2005, que acredita al Banco con los estándares más elevados de calidad y rigor profesional en la gestión de la seguridad de sus plataformas y sistemas informáticos, siendo la primera entidad financiera española en lograr esta certificación que avala una vez más el liderazgo de Bankinter en el ámbito de la tecnología, los sistemas de banca a distancia y la calidad de servicio a sus clientes.

La certificación del sistema de gestión de la seguridad de la información (SGSI) hace referencia a los procesos de "identificación, autenticación, firma de operaciones financieras y sus respectivas evidencias electrónicas a través del canal Internet". Para ello, la entidad ha sido sometida a una revisión exhaustiva de los aspectos organizativos y técnicos asociados a la gestión de la seguridad, sus procesos operativos para la detección y respuesta ante incidentes y su gestión del riesgo mediante un análisis riguroso, metodológico y periódico.

El proceso de implantación de todos los controles cubiertos en la norma ha requerido seis meses de trabajo del equipo de proyecto, si bien se han dedicado otros seis meses a la maduración del sistema, como requisito previo a la certificación. Todo ello pone de manifiesto el compromiso de Bankinter con la calidad, la seguridad, la mejora continua y la satisfacción del cliente.

Como característica diferencial del sistema de gestión de Bankinter, y en la opinión de los profesionales independientes que han participado en sus diferentes fases de validación, se encuentra "la plena integración de los procesos

[15] Fuente: Antecedente de implantación de un SGSI en una empresa nacional, extraído del siguiente enlace:
http://www.stakeholders.com.pe/index.php?option=com_content&task=view&id=2097

de gestión en el día a día de las áreas implicadas, garantizándose la continuidad y el correcto funcionamiento del sistema, así como que la gestión documental se realice totalmente en formato electrónico."

Este logro es coherente con la fuerte apuesta estratégica del Banco por los servicios de banca a distancia, especialmente Internet y el móvil, ámbitos en los que el Banco es pionero en Europa y un competidor claramente aventajado en el sector financiero. [16]

2.8.3 Comparación de soluciones

La ISO 27001:2005, es la única norma reconocida y certificable que especifica los requisitos para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización. Esta norma cubre todo tipo de organizaciones.

Es por ello que la Superintendencia de Bancos, Seguros y AFP (SBS), regula a las organizaciones financieras con ésta norma internacional ISO 27001, considerando gran parte de ella como obligatoria en la Circular Nº G-140.

[16] Fuente: Antecedente de instalación de un SGSI en una empresa extranjera, la información fue extraída de: http://www.eleconomista.es/empresas-finanzas/noticias/108827/11/06/Bankinter-recibe-la-certificacion-internacional-ISO-27001-para-sus-sistemas-de-seguridad-informatica.html

CAPÍTULO III
METODOLOGÍA

3.1 Recursos y metodologías

Se muestran los recursos y metodologías utilizadas para la elaboración del trabajo.

3.1.1 Recursos

RECURSOS SERVICIOS		
Nro.	**Descripción**	**Proveedor**
1	Especialista auditor PRICE para código fuente	PwC Perú
2	Curso de capacitación PRICE en pruebas unitarias	PwC Perú
3	DBA	-
4	Técnico electricista	-

RECURSOS HARDWARE/FÍSICOS		
Nro.	**Descripción**	**Proveedor**
1	Cisco Switch Catalyst WS-C6500	Cosapi Data, Japan Computer
2	Cisco Switch Catalyst WS-C2960G-48TC-L	Cosapi Data, Japan Computer
3	Patch Panel 48 puertos Panduit	Cosapi Data, Japan Computer
4	Repuestos PC Lenovo	IBM, Cosapi Data
5	Repuestos Laptops Lenovo	IBM, Cosapi Data
6	Racks para servidores Commscope	Cosapi Data, Japan Computer
7	Anexos Avaya	Fujita Comunicaciones
8	Licencias Avaya	Fujita Comunicaciones
9	Servidor Contingencia Avaya	Fujita

		Comunicaciones
10	Sistema de Control de Accesos	IP Solutions
11	Mecanismos de Encriptación SSL, SHH, VPN	-
12	Puerta de metal para Data Center	COSAPI
13	Extintores Amerex	Extintores Salvatore
14	Detector de Aniego Windland	Life Solutions
15	Detector de fuego Chemetron	Life Solutions
16	Extintor de Gas de Halotron Amerex	Life Solutions
17	Aire acondicionado de precisión Uniflair	SeguriCentro S.A.
18	Racks de comunicaciones Panduit, Commscope	Cosapi Data, Japan Computer
19	Muebles con seguridad	Cosapi
20	Módulos de comunicación	-
21	HSM ATALLA	Solnet
22	Solución IPS - Intrusion Prevention System McAfee, Cisco	Cosapi Data, Japan Computer
23	Control de temperatura	SeguriCentro S.A.
24	Deshumedesedor	SeguriCentro S.A.

RECURSOS SOFTWARE		
Nro.	**Descripción**	**Marca / Proveedor**
1	Software especializado para el control de versiones Subversion	-
2	Microsoft Sharepoint	Cosapi Data
3	Herramienta de encriptación GNU Privacy Guard, TrueCrypt	-
4	Software Especializado para el control de accesos	Sisbiocol CO, Accesor
5	Software Especializado para el monitoreo de Servidores Orion Solarwinds	Solarwinds
6	Servidores Virtuales Hyper-V	Cosapi Data
7	Software para replica de Storage	IBM
8	HA Storage	IBM
9	Herramienta de tráfico Orion Solarwinds	Solarwinds

RECURSOS SERVICIOS		
Nro.	**Descripción**	**Proveedor**
1	FTP GoAnywhere	-

RECURSOS MATERIALES		
Nro.	**Descripción**	**Proveedor**
1	Material de difusión para sensibilización	Tai Loy
2	Controles visuales	Copias Xpress

Cuadro 2.1: Recursos [17]

[17] Elaboración: los autores

3.1.2 Herramientas

3.1.2.1 Ciclo de Deming

El ciclo Deming es una herramienta de mejora continua. El ciclo consiste de una secuencia lógica de cuatro pasos repetidos que se deben de llevar a cabo consecutivamente. Estos pasos son:

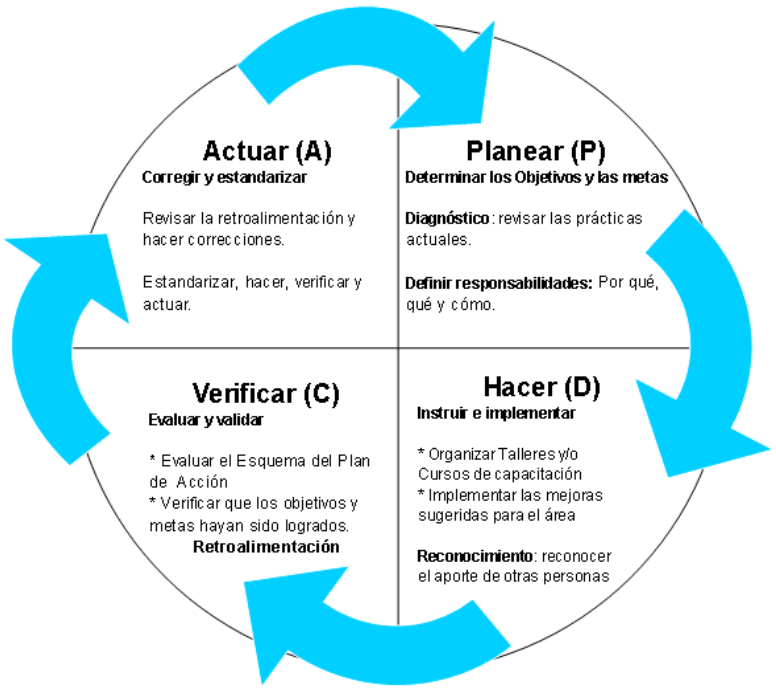


Gráfico 2.1: Ciclo Deming [18]

Los resultados de la implementación de este ciclo permiten a las empresas una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costes, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad de la empresa u organización.

[18] Fuente: El gráfico muestra los pasos seguidos en el ciclo Deming y fue extraído del siguiente enlace: http://www.monografias.com/trabajos35/atencion-cliente-ande/atencion-cliente-ande2.shtml

3.1.2.2 ISO/IEC 27001:2005

La ISO 27001:2005 está orientada a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las empresas, de amenazas externas o internas. La norma define a un Sistema de gestión de seguridad de información (SGSI) como:
"La parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar operar, monitorear, revisar, mantener y mejorar la seguridad de la información".

Es importante entender que la ISO/IEC 27001:2005 se ha desarrollado como modelo para el establecimiento, la implementación, la operación, el monitoreo, la revisión, el mantenimiento y la mejora de un SGSI para cualquier clase de organización. (Fuente www.slideshare.net)

3.1.2.3 ISO/IEC 27002:2005

"Código de prácticas para la gestión de la seguridad de la información". Es un modelo que da recomendaciones para las buenas prácticas. Es un modelo basado en el anexo A de la ISO/IEC 27001:2005, el cual amplia y explica de forma detalla como implantar los controles del anexo A de la ISO/IEC 27001:2005, este método no puede utilizarse para la certificación.

Gráfico 2.2: Dominios de la ISO/IEC 27002:2005 [19]

3.1.2.4 Diagrama de flujo BPMN

Es una notación gráfica que describe la lógica de los pasos de un proceso de negocio. Esta notación ha sido especialmente diseñada para coordinar la secuencia de los procesos y los mensajes que fluyen entre los participantes de las diferentes actividades, la cual consta de las siguientes características:

- Es un estándar internacional de modelado de procesos.
- Independiente de cualquier metodología de modelado de procesos.
- Crea un puente estandarizado para disminuir la brecha entre los procesos de la organización y la implementación de éstos.
- Permite modelar los procesos de manera unificada y estandarizada permitiendo un entendimiento a todas las personas de la organización.

3.1.2.5 Gestión de proyectos – PMBOK

La dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades de un proyecto para satisfacer los requisitos del proyecto. La dirección de proyectos se logra mediante la aplicación e integración de los procesos de dirección de proyectos de inicio, planificación, ejecución, seguimiento y control, y cierre. El director del proyecto es la persona responsable de alcanzar los objetivos del proyecto.

La dirección de un proyecto incluye:

- ✓ Identificar los requisitos
- ✓ Establecer unos objetivos claros y posibles de realizar
- ✓ Equilibrar las demandas concurrentes de calidad, alcance, tiempo y costes

[19] Fuente: El gráfico muestra los dominios de la ISO27002 y fue extraído del siguiente enlace: http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI/

- ✓ Adaptar las especificaciones, los planes y el enfoque a las diversas inquietudes y expectativas de los diferentes interesados.

Los directores del proyecto a menudo hablan de una “triple restricción” - alcance, tiempos y costes del proyecto - a la hora de gestionar los requisitos concurrentes de un proyecto. La calidad del proyecto se ve afectada por el equilibrio de estos tres factores. Los proyectos de alta calidad entregan el producto, servicio o resultado requerido con el alcance solicitado, puntualmente y dentro del presupuesto. La relación entre estos tres factores es tal que si cambia cualquiera de ellos, se ve afectado por lo menos otro de los factores. Los directores de proyectos también gestionan los proyectos en respuesta a la incertidumbre. El riesgo de un proyecto es un evento o condición inciertos que, si ocurre, tiene un efecto positivo o negativo al menos en uno de los objetivos de dicho proyecto.

El equipo de dirección del proyecto tiene una responsabilidad profesional ante sus interesados, incluidos los clientes, la organización ejecutante y el público. Los miembros de PMI acatan un “Código de Ética”, y quienes tienen la certificación de Profesional de la Dirección de Proyectos acatan un “Código de Conducta Profesional”.

- ➢ **Estructura de la Guía del PMBOK**

La Guía del PMBOK® está dividida en tres secciones.

- ✓ **Sección I: Marco Conceptual de la Dirección de Proyectos,** Marco Conceptual de la Dirección de Proyectos, proporciona una estructura básica para entender la dirección de proyectos.

  El capítulo 1, **Introducción**, define los términos clave y proporciona una descripción general del resto de la *Guía del PMBOK®.*

  El capítulo 2, **Ciclo de Vida del Proyecto y Organización** describe el entorno en el cual operan los proyectos. El equipo de dirección del proyecto debe comprender este amplio contexto.

La dirección de las actividades cotidianas del proyecto es necesaria, pero no suficiente para asegurar el éxito.

- ✓ **Sección II: Norma para la Dirección de Proyectos de un Proyecto**

  Norma para la Dirección de Proyectos de un Proyecto, especifica todos los procesos de dirección de proyectos que usa el equipo del proyecto para gestionar un proyecto.

  El capítulo 3, **Procesos de Dirección de Proyectos para un Proyecto**, describe los cinco grupos de Procesos de Dirección de Proyectos aplicables a cualquier proyecto y los procesos de dirección de proyectos que componen tales grupos. Este capítulo describe la naturaleza multidimensional de la dirección de proyectos.

- ✓ **Sección III: Áreas de Conocimiento de la Dirección de Proyectos**

  Áreas de Conocimiento de la Dirección de Proyectos, organiza los 44 procesos de dirección de proyectos de los Grupos de Procesos de Dirección de Proyectos del capítulo 3 en nueve áreas de conocimiento, según se describe a continuación. En la introducción de la sección III describe la leyenda de los diagramas de flujo de procesos que se usan en cada capítulo de Área de Conocimiento y en la introducción de todas las Áreas de conocimiento.

  El capítulo 4, **Gestión de la Integración del Proyecto**, describe los procesos y actividades que forman parte de los diversos elementos de la dirección de proyectos, que se identifican, definen, combinan, unen y coordinan dentro de los grupos de Procesos de Dirección de Proyectos.

  Se compone de los procesos de dirección de proyectos Desarrollar el Acta de Constitución del Proyecto, Desarrollar el Enunciado del Alcance del Proyecto Preliminar, Desarrollar el Plan de Gestión del Proyecto, Dirigir y Gestionar la Ejecución del

Proyecto, Supervisar y Controlar el Trabajo del Proyecto, Control Integrado de Cambios y cerrar proyecto.

El capítulo 5, **Gestión del Alcance del Proyecto**, describe los procesos necesarios para asegurarse de que el proyecto incluya todo el trabajo requerido, y solo el trabajo requerido, para completar el proyecto satisfactoriamente. Se compone de los procesos de dirección de proyectos planificación del alcance, definición del alcance, Crear EDT, verificación del alcance y control del alcance.

El capítulo 6, **Gestión del Tiempo del Proyecto**, describe los procesos relativos a la puntualidad en la conclusión del proyecto. Se compone de los procesos de dirección de proyectos definición de las actividades, establecimiento de la secuencia de las actividades, estimación de recursos de las actividades, estimación de la duración de las actividades, desarrollo del cronograma y control del cronograma.

El capítulo 7, **Gestión de los Costes del Proyecto**, describe los procesos involucrados en la planificación, estimación, presupuesto y control de costes de forma que el proyecto se complete dentro del presupuesto aprobado. Se compone de los procesos de dirección de proyectos
Estimación de costes, preparación del presupuesto de costes y control de costes.

El capítulo 8, **Gestión de la Calidad del Proyecto**, describe los procesos necesarios para asegurarse de que el proyecto cumpla con los objetivos por los cuales ha sido emprendido. Se compone de los procesos de dirección de proyectos planificación de calidad, realizar aseguramiento de calidad y realizar control de calidad.

El capítulo 9, **Gestión de los Recursos Humanos del Proyecto**, describe los procesos que organizan y dirigen el equipo del proyecto. Se compone de los procesos de dirección de proyectos planificación de los recursos humanos, adquirir el equipo del proyecto, desarrollar el equipo del proyecto y gestionar el equipo del proyecto.

El capítulo 10, **Gestión de las Comunicaciones del Proyecto,** describe los procesos relacionados con la generación, recogida, distribución, almacenamiento y destino final de la información del proyecto en tiempo y forma. Se compone de los procesos de dirección de proyectos planificación de las comunicaciones, distribución de la información, informar el rendimiento y gestionar a los interesados.

El capítulo 11, **Gestión de los Riesgos del Proyecto**, describe los procesos relacionados con el desarrollo de la gestión de riesgos de un proyecto. Se compone de los procesos de dirección de proyectos planificación de la gestión de riesgos, identificación de riesgos, análisis cualitativo de riesgos, análisis cuantitativo de riesgos, planificación de la respuesta a los riesgos, y seguimiento y control de riesgos.

El capítulo 12, **Gestión de las Adquisiciones del Proyecto**, describe los procesos para comprar o adquirir productos, servicios o resultados, así como para contratar procesos de dirección. Se compone de los procesos de dirección de proyectos planificar las compras y adquisiciones, planificar la contratación, solicitar respuestas de vendedores, selección de vendedores, administración del contrato y cierre del contrato.

- ✓ Áreas del conocimiento y procesos de la gestión de proyectos [20]

Áreas de Conocimiento	Grupos de Procesos				
	Inicio	Planeamiento	Ejecución	Control	Cierre
Gerencia de la Integración del Proyecto		Desarrollo del Plan del Proyecto	Ejecución del plan del Proyecto	Control Integrado del Cambio	
Gerencia del Alcance del Proyecto	Iniciación	Planeamiento del alcance		Verificación del alcance	
		Definición del alcance		Control del alcance del cambio	
Gerencia del Tiempo del Proyecto		Definición de actividades		Control de Horario	
		Secuencia de actividades			
Gerencia del Costo del Proyecto		Estimación de duración de actividades			Control del Costo
		Plantación de recursos			
		Estimación de Costos			
		Desarrollo del Presupuesto			
Gerencia de Calidad del Proyecto		Planeamiento de la calidad	Aseguramiento de la calidad	Control de Calidad	
Gerencia de los Recursos Humanos del Proyecto		Planeamiento Organizacional	Desarrollo de Equipo		
		Adquisición de Personal			
gerencia de Comunicación del Proyecto		Planeamiento de la comunicación	Distribución de la Información	Divulgación de reportes	
Gerencia de Riesgos del Proyecto	Planeamiento del manejo de riesgos			Monitoreo y control de riesgos	
	Identificación de riesgos				
	Análisis de riesgos cualitativos				
	Análisis de riesgos cuantitativos				
	Responsabilidad de riesgos				

[20] Fuente: Cuadro extraído del siguiente enlace:
http://www.comp.rgu.ac.uk/docs/ipoddev/mscitm/wimba/topic3/page_05.htm

3.1.2.6 Análisis de brechas

- Esta herramienta será usada para identificar las brechas entre el desempeño de la organización y el desempeño que se espera según la ISO 27001, con el fin de llevar a cabo en forma exitosa el modelo de gestión.
- El análisis de brechas es el examen detallado de la distancia existente entre cada elemento del diseño del SGSI y de la situación actual de la empresa.
- Las tácticas para cerrar las brechas son:
  - Ampliar el marco de tiempo para cumplir con el objetivo.
  - Reducir el tamaño o alcance del objetivo
  - Reasignar recursos para lograr las metas.
  - Obtener nuevos recursos.
- Cuando no se pueda cerrar la brecha
  - Si se evidencia que no hay posibilidad de cerrar una brecha, el equipo de planeación debe repetir el ciclo hasta el diseño de la estrategia del negocio y examinar el conjunto de metas en esta área
  - Se hace evidente que cada brecha se puede cerrar en forma individual, pero que en la realidad no es posible cerrarlas de manera simultánea, resulta necesario elegir varias alternativas. Repetir el ciclo entre el análisis de brechas y la reelaboración del modelo de la estrategia del negocio son mecanismos que se deben continuar hasta que surja uno que lleve claramente al logro exitoso.

3.1.3 Metodologías

Se utilizó como metodología para la gestión del proyecto la encontrada en el PMBOK y como metodología la gestión de riesgos una metodología elaborada por el grupo del proyecto basada en el MAGERIT y en la metodología de gestión de riesgos encontrada en el libro de Alexander, 2007.

3.1.3.1 Metodología para la gestión del proyecto

Esta metodología es la que se puede encontrar en el PMBOK, a continuación se procede a explicar las fases con las que cuenta y su adaptación para su uso en el trabajo presentado.

A) Iniciación

En esta primera fase para la gestión del proyecto, se facilita la autorización formal para comenzar el proyecto. Para ello se requiere:

- Levantar los requisitos de la organización,
- Evaluar las alternativas de solución,
- Se establecen descripciones claras de los objetivos del proyecto,
- Durante esta fase se define el alcance de manera preliminar y los recursos que la organización está dispuesta a invertir,
- Se elegirá al Jefe de Proyecto y al equipo de Proyecto.

Toda esta información se refleja en el **Acta de constitución el proyecto,** que una vez aprobado, el proyecto queda oficialmente autorizado.

 **Acta de constitución del proyecto**

B) Planificación del proyecto

En la segunda fase para la gestión del proyecto, se desarrolla el plan de gestión del proyecto. Este proceso también ayuda a identificar, definir y madurar el alcance del proyecto.

A medida que se obtiene nueva información sobre el proyecto, se identificarán nuevas dependencias, requisitos, riesgos, oportunidades, asunciones y restricciones. Para lograr ello se requiere:

- **Definición del alcance:** Proceso necesario para desarrollar el enunciado detallado del alcance del proyecto como base para las futuras decisiones del proyecto.

   **Alcance del proyecto**

- **Estructura de desglose de trabajo**: Proceso necesario para subdividir los principales productos entregables del proyecto y el trabajo del proyecto en componentes más pequeños y más fáciles de gestionar.

   **E.D.T.**

- **Cronograma del proyecto:** Es el proceso necesario para analizar las secuencias de las actividades, la duración de las actividades, los requisitos de los recursos y las restricciones del proyecto.

   **Cronograma de proyecto**

- **Planificación de recursos humanos**: Proceso necesario para identificar y documentar los roles dentro del proyecto, las responsabilidades y las relaciones de comunicación, así como para crear el plan de gestión de personal.

   **Organigrama**

- **Estimación de costes**: Proceso necesario para desarrollar una aproximación de los costes de los recursos necesarios

para completar todas las actividades del proyecto. Se realizará el estudio Costo/Beneficio.

Análisis costo/beneficio

- **Identificación de riesgos de proyecto**: Proceso necesario para determinar qué riesgos podrían afectar al proyecto y documentar sus características.

Evaluación de riesgos del proyecto

- **Planificación de la respuesta a los riesgos del proyecto**: Proceso necesario para desarrollar operaciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

Respuesta de los riesgos del proyecto

C) Ejecución del proyecto

Esta tercera fase se compone de todos los entregables definidos en el cronograma del proyecto, a fin de cumplir con los requisitos del proyecto.

- **Gestionar la ejecución del proyecto:** Proceso necesario para dirigir las diversas interfaces técnicas y de la organización que existen en el proyecto a fin de ejecutar el trabajo definido en el Cronograma del Proyecto. Los productos entregables son producidos como salidas.
- **Selección de proveedores:** Proceso necesario para analizar ofertas, seleccionando entre los posibles vendedores y negociando un contrato por escrito con el vendedor.

Matriz de selección de proveedores

D) Seguimiento y control

- **Seguimiento a las actividades programadas**: Proceso necesario para recoger, medir y difundir información sobre el rendimiento del proyecto, y para evaluar las mediciones y tendencias del mismo.

 **Seguimiento mensual del proyecto**

- **Control de cambios:** Proceso necesario para controlar los factores que producen cambios, a fin de asegurarse de que esos cambios no perjudiquen el estado del proyecto.

 **Control de cambios**

E) Cierre

- **Cierre del proyecto:** Proceso necesario para finalizar las actividades de todos los procesos a fin de cerrar formalmente el proyecto.

 **Acta de cierre de proyecto**

3.1.3.2 Metodología para el Diseño e Implementación de un SGSI (MEDIS)

La siguiente es una metodología desarrollada por el equipo del proyecto tomando como referencias a la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) y la metodología de análisis y gestión de riesgos presentada en el libro de Alexander, 2007.

A) Política de SGSI

La Política de SGSI es una declaración de la Gerencia que se define teniendo en consideración:

- Debe incluir el marco referencial para establecer los objetivos,

- Debe tomar en cuenta los requerimientos comerciales, legales, reguladores, y las obligaciones de la seguridad contractual,
- Debe estar alineada con el contexto de la gestión del riesgo estratégico de la gerencia,
- Debe establecer el criterio con el que se evalúa el riesgo,
- Debe ser revisada y aprobada por la gerencia.

B) Manual del SGSI

Para la elaboración del manual se debe tener en consideración lo siguiente:

- El manual del SGSI debe proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI,
- Se debe definir el alcance aplicable,
- Se debe definir responsabilidades de cumplimiento y ejecución.

C) Análisis de brechas

El análisis de brechas se debe elaborar, comparando el estado actual de la organización con los requisitos obligatorios indicados en la Circular N° G-140 de la SBS.

Para dicho análisis se debe realizar un estudio a los procesos actuales de la organización, donde se incluirá el porcentaje de cumplimiento para cada dominio obligatorio de la Circular N° G-140, siguiendo el siguiente formato:

Ítem	Requisitos Circular G-140	Cumple	Nivel Cumplimiento
Generalidades			
Seguridad lógica			
Seguridad de personal			
Seguridad física ambiental			
Inventario de activos y clasificación de la información			
Administración de las operaciones y comunicaciones			
Adquisición, desarrollo y mantenimiento de sistemas informáticos			

Procedimientos de respaldo
Gestión de incidentes de seguridad de información

Cuadro 3.1: Análisis de brechas [21]

D) Análisis y evaluación de riesgos [22]

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- **(1)** Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- **(2)** Determinar a qué amenazas están expuestos aquellos activos.
- **(3)** Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- **(4)** Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- **(5)** Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se tratan primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las estimaciones de impacto y riesgo sean "potenciales": caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

[21] Elaboración: los autores.

[22] Fuente: Metodología elaborada por el equipo de proyecto, la cual está basada en las mejores prácticas de metodologías como Magerit y del libro: Diseño de un sistema de gestión de seguridad de información, Alexander (2007).

Gráfico 2.6: Elementos del riesgo [23]

a) Identificación de procesos

Como primer paso se deben identificar todos los procesos que se encuentran dentro del alcance del SGSI y representarlos con diferentes herramientas; tales como: procedimientos, instructivos, caracterización, fichas, cartillas, etc.

Diagrama de procesos

b) Identificación de activos

Para la identificación de los activos se utiliza el método de las elipses. Esta metodología permite, con gran precisión, poder identificar los activos de información.

Lo primero que se debe hacer es determinar en la elipse concéntrica, los distintos procesos y subprocesos que están incluidos dentro del alcance del SGSI. A cada proceso se le identificaron sus respectivos subprocesos.

El segundo paso consiste en identificar en la elipse intermedia las distintas interacciones que los procesos de la elipse concéntrica tienen las diferentes áreas de la organización. Seguidamente, en la elipse externa, se identifican aquellas organizaciones extrínsecas a la empresa que tienen cierto tipo de interacción con los procesos y subprocesos identificados en la elipse concéntrica.

[23] Fuente: Gráfico que muestra la interrelación entre los elementos del riesgos, fue extraído del siguiente enlace: http://cata-seguridaddelainformacion.blogspot.com/

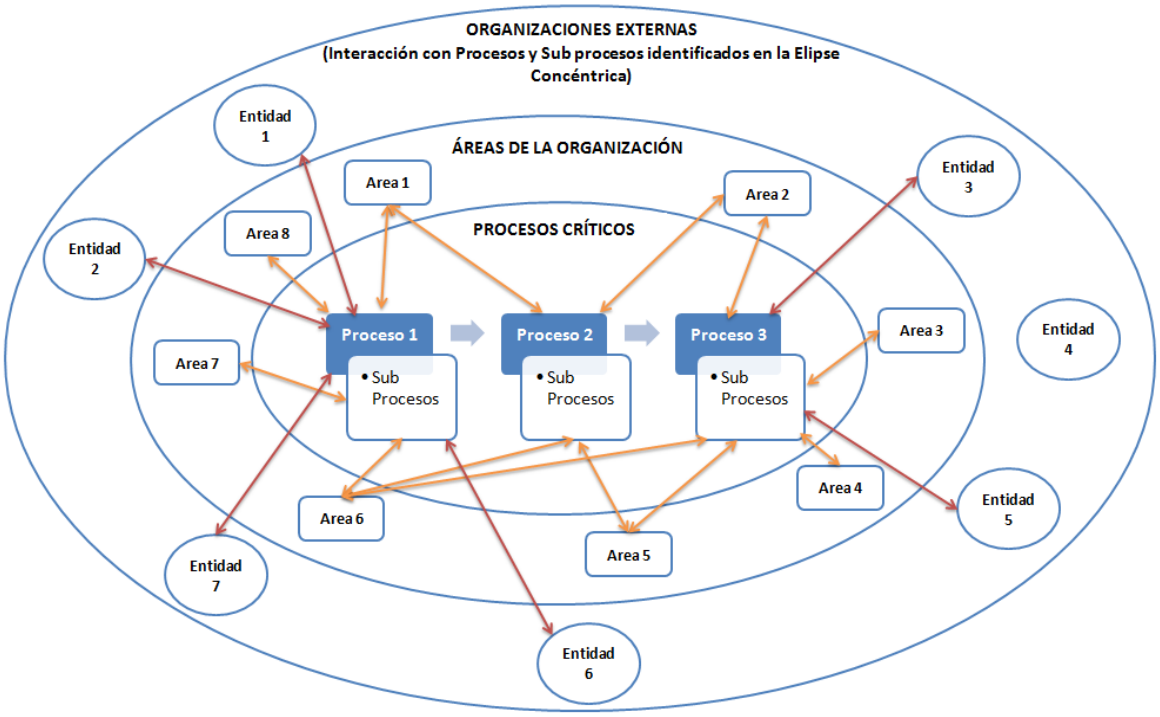


Gráfico 2.7: Método de las elipses [24]

El método de las elipses se utiliza como fuente de inspiración para derivar, posteriormente, al **documento de análisis para la identificación activos de información**, ya que, al analizar los procesos identificados y el flujo de información con las áreas y las entidades extrínsecas, se procede a identificar todos los activos de información que serán representados en el **documento inventario de activos de seguridad de información.**

Identificación de activos (elipses)

c) Inventario de activos

Para la elaboración del **documento inventario de activos de seguridad de información**, se debe tener en consideración lo siguiente, para la categorización de los Activos de Información:

CATEGORÍAS DE ACTIVOS			
TIPO	**CÓDIGO**	**CATEGORÍA**	**EJEMPLO**

[24] Elaboración: los autores.

Activos de información	**I1**	Información electrónica	Base de datos y documentos creados y o conservados en medios electrónicos (correo electrónico, audio, video, entre otros).
	I2	Información escrita	Documentos creados y o conservados en papel.
	I3	Información hablada	Conversaciones presenciales, telefónicas, presentaciones orales o a través de medios virtuales (video conferencia).
	I4	Otro tipo de información	-
Activos de software	**SW0**	Software base o sistema operativo	Software Base o Sistema Operativo Windows 2000, Windows XP, Windows 2000 server, Windows 2003 server, Linux, Unix, etc.
	SW1	Software comercial o herramientas, utilitarios	Office, Adobe, Primo, entre otros.
	SW2	Software desarrollado por terceros	SAP, JD Edwards, Oracle
	SW3	Software desarrollado internamente	Sistema Integrado, Aplicativo, Modulo de Sistema, etc
	SW4	Software de administración de Base de Datos	SQL, Oracle, DB/2, Informix, etc.
	SW5	Otro software	-
Activos de hardware	**F1**	Equipo de procesamiento	Servidores, computadoras, laptops, entre otros.
	F2	Equipo de comunicaciones	Routers, centrales digitales, máquinas de fax, entre otros.
	F3	Medio de almacenamiento	Discos, cintas, disquetes, CD 's, DVD's, memorias USB, entre otros.
	F4	Mobiliario y equipamiento	Estantes, cajas fuertes, archivadores, entre otros.
	F5	Otros equipos	Impresoras, fotocopiadoras, scanners, entre otros
Servicios (Terceros)	**S1**	Procesamiento y comunicaciones	Servicio de Procesamiento de la información, de impresión, de fotocopiado, de mensajería, telefonía fija y celular, entre otros.
	S2	Servicios generales	Calefacción, energía eléctrica, aire acondicionado, entre otros.
	S3	Otros servicios	Servicio de intermediación laboral, entre otros.

Cuadro 3.2: Inventario de activos [25]

Para todos los activos de información deben existir siempre:

- **Usuario:** Rol que emplea el activo de información para su trabajo.
- **Responsable:** Rol que es dueño del activo de información.
- **Custodio: Rol** que custodia los activos de información.

Todos los activos de información inventariados deben tener ser valorizados según el siguiente cuadro:

d) Análisis y evaluación de riesgos

- **Identificación de amenazas** [26]

Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos de información y causar un daño.

Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y sus activos.

Para una empresa, las amenazas pueden ser de distintos tipos con base en su origen.

[25] Elaboración: los autores.

[26] Fuente: Cuadro creado por el grupo de proyecto para indicar el valor de un activo de información.

VALOR DEL ACTIVO	**Alto**	Cuando la destrucción, modificación, revelamiento o interrupción de la información afecta **seriamente** la operatividad, competitividad, rentabilidad o imagen de la organización.
	Medio	Cuando la destrucción, modificación, revelamiento o interrupción de la información afecta **considerablemente** la operatividad, competitividad, rentabilidad o imagen de la organización.
	Bajo	Cuando la destrucción, modificación, revelamiento o interrupción de la información **no afecta considerablemente** la operatividad, competitividad, rentabilidad o imagen de la organización.

Cuadro 3.3: Valoración de activos [27]

- ✓ **Clasificación de amenazas**
  - Amenazas naturales (inundaciones, sismos, incendios, tormentas, etc)
  - Amenazas a instalaciones (energía, explosión, fuego, fallas, etc)
  - Amenazas humanas (transporte, renuncias, huelgas, accidentes, etc)
  - Amenazas tecnológicas (virus, hacking, red, fallas software hardware)
  - Amenazas operacionales (crisis, legal, fallas equipos, proveedores)
  - Amenazas sociales (motines, protestas, vandalismo, violencia, etc)

Inventario de activos

- ✓ **Identificación de amenazas y mecanismos de protección**

Una vez determinada que una amenaza puede perjudicar a un activo, hay que estimar si afecta a la confidencialidad, integridad y disponibilidad del SGSI.

[27] Elaboración: los autores

La organización puede contar con mecanismos de protección los cuales reducen la probabilidad de ocurrencia de dichas amenazas. Se deben identificar los mecanismos de protección actual clasificada en:

- **Preventivos**: Mecanismo de protección que previene a que la amenaza se materialice.
- **Detectivos**: Mecanismo de protección que detecta cuando una amenaza se materializa.
- **Correctivos**: Mecanismo de protección que ejecutará después que la amenaza se haya materializado.

- **Identificación de vulnerabilidades**

Las vulnerabilidades son debilidades de seguridad asociadas a los activos de información de una organización.

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño. Simplemente son condiciones que pueden hacer que una amenaza se materialice y afecte un activo.

Es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos. Por esta razón es necesario entender la relación entre amenazas y vulnerabilidades. La pregunta fundamental es ¿Qué amenaza pudiese explotar cuál de las vulnerabilidades?

- ✓ **Clasificación de vulnerabilidades**
  - Seguridad lógica
  - Seguridad de recursos humanos
  - Seguridad física y ambiental
  - Seguridad gestión de operaciones y comunicaciones
  - Mantenimiento, desarrollo y adquisición de sistemas de información

- **Determinación del impacto / probabilidad** [28]

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

El impacto mide el daño causado por un incidente en el supuesto de que ocurriera.

La frecuencia pone en perspectiva aquel impacto, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acumular un daño considerable.

Tomando en consideración las amenazas, mecanismos de protección actuales y las vulnerabilidades del sistema de seguridad para todos los activos de información se debe definir:

- La **valoración** de los activos, que es la sumatoria del impacto del activo en la **confidencialidad**, **integridad** y **disponibilidad** del SGSI, en una escala del 1(Muy Bajo) al 5 (Muy Alto).
- La **probabilidad** que las amenazas se materialicen, usando la siguiente clasificación:

5: Muy Alto	Ocurrencia diaria
4: Alto	Ocurrencia semanal
3: Medio	Ocurrencia mensual
2: Bajo	Ocurrencia anual
1: Muy bajo	Ocurrencia en dos años a más

Cuadro 3.4: Probabilidad de materialización de amenazas [29]

- **Impacto** que ocasionaría el que las amenazas se materialicen, usando la siguiente clasificación:

[28] Fuente: Cuadros elaborados por el grupo de proyecto para asignarle valores de ocurrencia y como afecta al negocio que una amenaza se materialice sobre un activo de información.
[29] Elaboración: los autores

5: Muy Alto	- Afecta a los socios - Afecta a los establecimientos - Afecta a los partners - Afecta a entidades regulatorias
4: Alto	- Afecta a más de un área de la empresa
3: Medio	- Afecta a un usuario, no hay posibilidad de trabajo alterno
2: Bajo	- Afecta a un usuario, existe posibilidad de trabajo alterno
1: Muy bajo	- No afecta a la productividad

Cuadro 3.5: Impacto que ocasiona una amenaza al materializarse [30]

- **Determinación del riesgo**

El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la probabilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

Valoración = C + I + D

Riesgo = Probabilidad * Impacto + Valoración

Los riesgos no se pueden eliminar, solo mitigar, es por ello que se establece un nivel de tolerancia de riesgos, expresado en:

Totalmente Tolerable: TT	**4 – 15**
Regularmente Tolerable: RT	**16 – 25**
No Tolerable: NT	**26 – 40**

Para activos que tienen **mínimo** un riesgo que resulte **regularmente tolerable** o **no tolerable** se debe re-definir salvaguardas.

Los riesgos que resulten Totalmente Tolerable, son opcionales para ser tratados.

[30] Elaboración: los autores

e) Gestión del riesgo

- **Definición de salvaguardas**

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se evitan simplemente organizándose adecuadamente, otras requieren elementos técnicos, otra seguridad física y por último, están las políticas de personal.

Las salvaguardas se caracterizan por su eficacia frente al riesgo que pretenden mitigar. La salvaguarda ideal es 100% eficaz, lo que implica que:

- Es teóricamente idónea
- Está perfectamente desplegada, configurada y mantenida
- Se emplea siempre
- Existen procedimientos claros de uso normal y en caso de incidencias
- Los usuarios están formados y concientizados
- Existen controles que avisan de posibles fallos.

Las estrategias para el tratamiento de las salvaguardas pueden ser:

- **Reducción del riesgo (R):** Para todos aquellos riesgos donde la opción de reducirlos se ha tomado, se deben implementar controles apropiados para poder reducirlos a un nivel aceptable.
- **Aceptar el riesgo (A):** Muchas veces se presentan situaciones en la cual la organización no encuentra controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias, la decisión de aceptar el riesgo y vivir con las consecuencias es la más adecuada.
- **Transferencia del riesgo (T):** La transferencia del riesgo es una opción cuando para la compañía es difícil reducir o controlar el

riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante estas circunstancias.

- **Evitar el riesgo (E):** Es cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad en particular, para así evitar la presencia del riesgo.
- Por cualquiera de las estrategias que se opte, todas las salvaguardas incurren en un costo y tiempo que estarán gestionados por el/los responsables de implementación.
- Para dimensionar el **costo aproximado** de la implantación de la salvaguarda elegida, se considera:

3	Alto costo
2	Medio costo
1	Bajo costo
D	Desconocido

- Para dimensionar el **tiempo aproximado** de la implantación de la salvaguarda elegida, se considera:

C	Corto plazo (Menos de 1 meses)
M	Mediano plazo (De 1 a 2 meses)
L	Largo plazo (Más de 3 meses)
D	Desconocido

- **Determinación del riesgo residual**

Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia.

Riesgo Residual = Probabilidad R. * Impacto R. + Valoración

Totalmente tolerable: TT	**4 – 15**
Regularmente tolerable: RT	**16 – 25**
No tolerable: NT	**26 – 40**

Cuadro 3.6: Medición del impacto y probabilidad del riesgo [31]

Para los riesgos que resulten nuevamente r**egularmente tolerable** o **no tolerable** se debe re-definir nuevamente salvaguardas.

Los riesgos que resulten **totalmente tolerables**, son considerados **riesgos despreciables**, y no requieren más acciones, que el monitoreo periódico.

Tratamiento de riesgos

E) Plan de tratamiento de riesgos

La organización debe:

- Formular el plan de tratamiento de riesgo que identifique las acciones apropiadas, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.
- Implementar el plan de tratamiento de riesgos para poder lograr los objetivos, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.

Plan de tratamiento de riesgos

[31] Elaboración: los autores

3.2 Desarrollo del proyecto

3.2.1 Gestión del proyecto SGSI

3.2.1.1 Iniciación

A) Acta de constitución del proyecto [32]

Hoy, 09 de octubre del 2011, se constituye el **Comité del SGSI** conformado por:

Cargo	Dependencia	Firma
Gerencia de Tecnología	Gerencia de Tecnología	
Sub Gerente Tecnología	Gerencia de Tecnología	
Jefe de Centro de Cómputo	Gerencia de Tecnología	
Coordinador de BI	Gerencia de Tecnología	
Jefe de Riesgo Operacional	Gerencia de Riesgos	

Asimismo, se constituye también el **Equipo Implementador SGSI** conformado por:

Cargo	Dependencia	Firma
Jefe de Centro de Cómputo	Gerencia de Tecnología	
Coordinador de BI	Gerencia de Tecnología	
Jefe de Producción	Jefatura de Centro de Cómputo	
Jefe de Proyectos	Jefatura de Desarrollo	
Jefe de Riesgo Operacional	Gerencia de Riesgos	
Jefe de Proyecto SGSI	Gerencia de Tecnología	
Consultor SGSI	Gerencia de Tecnología	

Mediante la presente, el **comité del SGSI** y el **equipo implementador SGSI** asumen el compromiso de participar de manera directa en la implementación del Proyecto "**Implementación del SGSI en la gerencia de tecnología**", establecido por la Gerencia de Tecnología de Card Perú S.A, para el cual contarán con responsabilidades establecidas en el **manual de funciones del SIG.**

[32] Fuente: Cuadros creados por el grupo de proyecto para indicar el cargo y dependencias de las personas involucradas en el proyecto.

La implementación de este sistema permite identificar, analizar, evaluar, controlar y/o mitigar los riesgos a los que están expuestos todos los activos de Tecnologías de Información.

Se define el alcance del proyecto para todos los procesos que se encuentran bajo la Gerencia de Tecnología, los cuales son:

- Procesos de Centro de Cómputo
- Procesos de Business Intelligence
- Procesos de Desarrollo

Fecha inicio de proyecto: 09 de octubre del 2011
Sponsor del proyecto : Gerente de Tecnología
Representante del SGSI : Jefe de Centro de Cómputo
Facilitador del SGSI : Carlos Barrantes / Javier Hugo
Horario de reuniones :

Centro Cómputo	Martes : 11:00 – 01:00 PM
B.I.	Lunes : 02:00 – 04:00 PM
Desarrollo	Lunes : 04:00 – 06:00 PM

3.2.1.2 Planificación del proyecto

A) Alcance del proyecto [33]

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
Diseño e implementación de un SGSI para los procesos de tecnología de Card Perú S.A.	**DI-SGSI-TEC**

JUSTIFICACIÓN DEL PROYECTO
Debido a los riesgos a los que están expuestos los activos de información, el impacto que la interrupción de estos puede causar, ya sea pérdida de información o financiera; es preponderante la definición de una metodología y el uso de herramientas que nos ayuden reducir y mitigar estos riesgos. Es por ello que se propone la implementación de un Sistema de Gestión de Seguridad de Información (SGSI), el cual nos brindará los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información, implantar los controles necesarios que ayudarán a salvaguardar los activos de información de los procesos de tecnología, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de Información (SGSI), alineándolo de esta manera a los objetivos estratégicos de la organización.
DESCRIPCIÓN DEL PRODUCTO
Implementación de un Sistema de Gestión de Seguridad de Información enfocado a los procesos de tecnología, basado en la ISO 27001:2005.
ENTREGABLES DEL PROYECTO
Los entregables de todo el proyecto son especificados en la “Estructura de Desglose de Trabajo” (Ver 3.2.1.2.2)

[33] Elaboración: los autores

ALCANCE

El proyecto se ejecutará en la empresa Card Perú S.A. donde se realizará la implementación de un Sistema de Gestión de Seguridad de Información (SGSI) enfocado a los “Procesos de Tecnología”, los cuales son:

- Atención de requerimientos
- Desarrollo de soluciones tecnológicas
- Control de calidad de soluciones tecnológicas
- Gestión de proyectos
- Planificación del mantenimiento de HW y SW
- Procesamiento de Información
- Operación de seguridad de la información
- Investigación tecnológica

FUERA DEL ALCANCE

Los procesos estratégicos, operativos y los procesos de apoyo, tales como: Gestión de la Documentación, Gestión de Recursos Humanos, Gestión Administrativa, Gestión Internacional, Gestión Financiera Contable.

ORGANIZACIÓN DEL PROYECTO

- Sponsor de Proyecto
- Jefe de Proyecto SGSI
- Consultor Sr. de SGSI
- Gerente de Tecnología
- Sub Gerente de Tecnología
- Coordinador de Business Intelligence
- Jefe de Riesgo Operacional
- Jefe de Producción
- Coordinador de Networking
- Jefe de Proyectos
- Desarrollador B.I.

OBJETIVO DE CRONOGRAMA

-Fecha de Inicio: 07/11/2011

-Fecha de Fin: 22/06/2012

-Cumplir con las fechas establecidas, siendo medidas con % de avance.

B) Estructura de desglose de trabajo

A3

C) Cronograma del proyecto [34]

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1	**DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN PROCESOS TECNOLÓGICOS**	**185 días**	**lun 10/10/11**	**vie 22/06/12**		
2	**Gestión del proyecto**	**185 días**	**lun 10/10/11**	**vie 22/06/12**		
3	**Iniciación**	**1 día**	**lun 10/10/11**	**lun 10/10/11**		
4	Elaborar el acta de constitución del proyecto	1 día	lun 10/10/11	lun 10/10/11		CBarrantes
5	**Planificación del proyecto**	**8 días**	**mar 11/10/11**	**jue 20/10/11**		
6	Elaborar alcance del proyecto	1 día	mar 11/10/11	mar 11/10/11	4	CBarrantes
7	Aprobación del alcance del proyecto (reunión)	2 días	mié 12/10/11	jue 13/10/11	6	CBarrantes
8	Identificar entregables según alcance del proyecto	1 día	vie 14/10/11	vie 14/10/11	7	CBarrantes
9	Elaborar EDT	1 día	vie 14/10/11	vie 14/10/11		CBarrantes
10	Estructurar cronograma del proyecto	1 día	lun 17/10/11	lun 17/10/11	8	CBarrantes
11	Identificar responsables de proyecto / elaborar organigrama	1 día	mar 18/10/11	mar 18/10/11	10	CBarrantes
12	Elaborar análisis costo/beneficio	1 día	mié 19/10/11	mié 19/10/11	11	CBarrantes
13	Identificar los riesgos que afectan al proyecto	1 día	mié 19/10/11	mié 19/10/11		CBarrantes
14	Identificar un plan de tratamiento de riesgos	1 día	jue 20/10/11	jue 20/10/11	13	CBarrantes
15	**Ejecución del proyecto**	**176 días**	**vie 21/10/11**	**vie 22/06/12**		
16	Estructurar propuesta de política del SGSI	2 días	vie 21/10/11	lun 24/10/11	14	CBarrantes
17	Elaborar despliegue de política	3 días	mar 25/10/11	jue 27/10/11	16	CBarrantes
18	Elaborar manual del SGSI	1 día	vie 28/10/11	vie 28/10/11	17	CBarrantes
19	Identificar brechas entre circular N° G-140 y la realidad de la empresa	1 día	lun 31/10/11	lun 31/10/11	17	JHugo
20	Elaborar informe de brechas PRE	5 días	mar 01/11/11	lun 07/11/11	19	JHugo
21	**Análisis y evaluación de riesgos**	**36 días**	**mar 01/11/11**	**mar 20/12/11**		
22	Elaborar diagrama de identificación de procesos de centro de cómputo, desarrollo y B.I.	11 días	mar 01/11/11	mar 15/11/11		CBarrantes
23	**Departamento de centro de cómputo**	**26 días**	**mar 15/11/11**	**mar 20/12/11**		
24	Identificar los procesos - subprocesos - procedimientos (inventario)	5 días	mar 15/11/11	lun 21/11/11		JHugo
25	Identificación de activos por procesos - subprocesos - procedimientos	7 días	mar 22/11/11	mié 30/11/11	24	JHugo
26	Valoración e inventario de activos identificados.	3 días	jue 01/12/11	lun 05/12/11	25	JHugo
27	Identificar y evaluar amenazas por activos identificados.	5 días	mar 06/12/11	lun 12/12/11	26	JHugo
28	Identificar y evaluar riesgos (importancia) por activos identificados.	6 días	mar 13/12/11	mar 20/12/11	27	JHugo
29	**Departamento de desarrollo**	**26 días**	**mar 15/11/11**	**mar 20/12/11**		
30	Identificar los procesos - subprocesos - procedimientos (inventario)	5 días	mar 15/11/11	lun 21/11/11		CBarrantes
31	Identificación de activos por procesos - subprocesos - procedimientos	7 días	mar 22/11/11	mié 30/11/11	30	CBarrantes
32	Valoración e inventario de activos identificados.	3 días	jue 01/12/11	lun 05/12/11	31	CBarrantes

[34] Elaboración: los autores

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
33	Identificar y evaluar amenazas por activos identificados.	5 días	mar 06/12/11	lun 12/12/11	32	CBarrantes
34	Identificar y evaluar riesgos (importancia) por activos identificados.	6 días	mar 13/12/11	mar 20/12/11	33	CBarrantes
35	**Departamento de business intelligence**	**26 días**	**mar 15/11/11**	**mar 20/12/11**		
36	Identificar los procesos - subprocesos - procedimientos (inventario)	5 días	mar 15/11/11	lun 21/11/11		JHugo
37	Identificación de activos por procesos - subprocesos - procedimientos	7 días	mar 22/11/11	mié 30/11/11	36	JHugo
38	Valoración e inventario de activos identificados.	3 días	jue 01/12/11	lun 05/12/11	37	JHugo
39	Identificar y evaluar amenazas por activos identificados.	5 días	mar 06/12/11	lun 12/12/11	38	JHugo
40	Identificar y evaluar riesgos (importancia) por activos identificados.	6 días	mar 13/12/11	mar 20/12/11	39	JHugo
41	Hallar el riesgo efectivo por amenaza de un activo	4 días	jue 05/01/12	mar 10/01/12		JHugo
42	Definir controles de implementación	11 días	mié 11/01/12	mié 25/01/12	41	JHugo
43	Revisiones de controles propuestos	3 días	jue 26/01/12	lun 30/01/12	42	JHugo
44	Definir Plan de acción de tratamiento del riesgo	4 días	mié 01/02/12	lun 06/02/12	43	Equipo SGSI
45	Estudio y selección de proveedores	4 días	mar 07/02/12	vie 10/02/12	44	Equipo SGSI
46	Implementación del plan de tratamiento del riesgo desarrollo	89 días	mar 07/02/12	vie 08/06/12	44	Equipo SGSI
47	Implementación del plan de tratamiento del riesgo centro computo	89 días	mar 07/02/12	vie 08/06/12	44	Equipo SGSI
48	Implementación del plan de tratamiento del riesgo business intelligence	89 días	mar 07/02/12	vie 08/06/12	44	Equipo SGSI
49	Implementación del plan de tratamiento del controles - Brecha circular Nª G-140	30 días	mar 07/02/12	lun 19/03/12	44	Equipo SGSI
50	Identificar documentos necesarios/obligatorios	4 días	lun 30/04/12	jue 03/05/12		Equipo SGSI
51	Elaborar Programa de capacitación y concientización	1 día	vie 04/05/12	vie 04/05/12		CBarrantes
52	Elaborar material de capacitación y concientización	4 días	lun 07/05/12	jue 10/05/12	51	CBarrantes
53	Coordinar fechas para la capacitación y concientización	1 día	vie 25/05/12	vie 25/05/12		CBarrantes
54	Ejecutar capacitación y concientización a personal involucrado	6 días	vie 01/06/12	vie 08/06/12	53	CBarrantes
55	Elaborar evaluación de SGSI	6 días	vie 01/06/12	vie 08/06/12		JHugo
56	Evaluar a los participantes de la capacitación y concientización	6 días	vie 01/06/12	vie 08/06/12		JHugo
57	Calificar evaluaciones	6 días	vie 01/06/12	vie 08/06/12		JHugo
58	Presentar resultados de capacitación y concientización a gerencia	1 día	lun 11/06/12	lun 11/06/12	57	JHugo
59	Elaboración del análisis de brechas POST (Informe)	3 días	lun 11/06/12	mié 13/06/12		CBarrantes
60	Resultado y análisis de indicadores	2 días	jue 14/06/12	vie 15/06/12	59	CBarrantes
61	Presentar resultados finales a gerencia	1 día	vie 22/06/12	vie 22/06/12		CBarrantes
62	**Seguimiento y control**	**166 días**	**vie 21/10/11**	**vie 08/06/12**		
63	Registro de avances mensuales	166 días	vie 21/10/11	vie 08/06/12		CBarrantes
64	Registro de cambios del proyecto	149 días	mar 15/11/11	vie 08/06/12		CBarrantes
65	**Cierre**	**1 día**	**vie 22/06/12**	**vie 22/06/12**		
66	Elaborar el acta de cierre de proyecto	1 día	vie 22/06/12	vie 22/06/12	64	CBarrantes

D) Organigrama

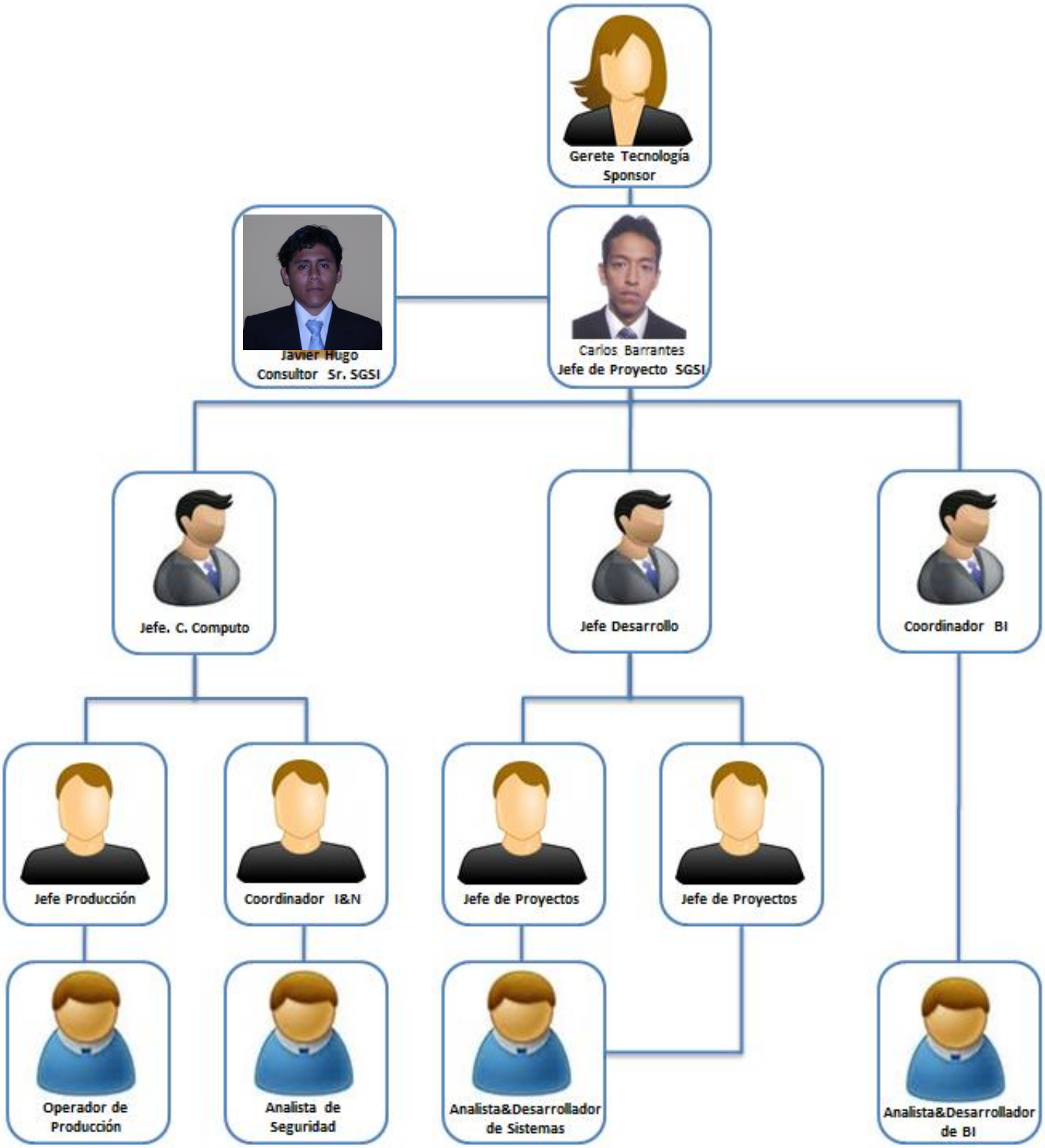


Gráfico 2.8: Organigrama [35]

E) Análisis costo / beneficio

Costos de implementación de SGSI		
Descripción	**Precio (S/.)**	**Tiempo de vida (Años)**
Jefe de Proyecto	40000	1
Consultor SGSI	32000	1
Especialista Auditor PRICE para código fuente	10000	1
DBA	5000	1
Curso de capacitación PRICE en pruebas unitarias	5000	1
Técnico electricista	5000	1
Cisco Switch Catalyst WS-C6500	52200	5
Cisco Switch Catalyst WS-C2960G-48TC-L	57420	5
Patch Panel 48 puertos Panduit	24000	5
Repuestos PC Lenovo	5000	3
Repuestos Laptops Lenovo	6000	3
Racks para servidores Commscope	6000	3
Anexos Avaya	1500	6
Licencias Avaya	4500	1
Servidor Contingencia Avaya	6000	5
Sistema de Control de Accesos	5000	3
Mecanismos de Encriptación SSL, SHH, VPN	1000	1
Puerta de metal para Data Center	800	3
Extintores Amerex	1000	3
Detector de Aniego Windland	2000	3
Detector de fuego Chemetron	1500	3
Extintor de Gas de Halotron Amerex	1500	3
Aire acondicionado de precisión Uniflair	2500	5
Racks de comunicaciones Commscope	6000	3
Muebles con seguridad	2000	5
HSM ATALLA	35000	5
Solución IPS - Intrusion Prevention System McAfee, Cisco	3500	5
Control de temperatura	700	5
Deshumedesedor	500	5
Software Especializado para el control de versiones Subversion	300	1
Microsoft Sharepoint	400	1
Herramienta de encriptación GNU Privacy Guard	200	1
Software Especializado para el control de accesos	500	1

[35] Fuente: Gráfico creado por el grupo de proyecto para establecer la organización del proyecto.

Software Especializado para el monitoreo de Servidores Orion Solarwinds	6500	1
Servidores Virtuales Hyper-V	400	1
Software para replica de Storage	700	1
HA Storage	5000	1
Herramienta de tráfico Orion Solarwinds	3000	1
FTP GoAnywhere	200	1
Material de difusión para sensibilización	-	-
Controles visuales	-	-
Costo Total (S/.)	**339 820.00**	

Cuadro 3.7: Análisis costo/beneficio [36]

Ahorro supuesto anual por contar con un SGSI	
Descripción	**Ahorro**
Pérdida de información accidental	100 000
Pérdida de información por desastres naturales y/o provocados	250 000
Pérdida o robo de información por problemas de comunicación	50 000
Interrupción de los procesos core de negocio (2)	1000 000
Robo de información de los clientes, personal interno, contratistas y/o proveedores	50 000
Total ahorro supuesto anual (S/.)	**1 450 000**
Ingresos Card Perú S.A. - 2011	**400 000 000**

S/.	**401 450 000**

Cuadro 3.8: Ahorro anual por contar con un SGSI [37]

Beneficio	:	**1 450 000**
Costo	:	**339 820**
B/C	:	**4.26696486**

Meses	:	**12**
B/C	:	**2.81230345**
Tiempo Recuperación:		**3 meses**

El tiempo de recuperación de la inversión del Proyecto SGSI puede variar dependiendo de cuantos incidentes reales sucedan al año.

En este supuesto, se consideró que pasó al menos una vez al año cada uno de los incidentes.

[36] Elaboración: los autores
[37] Elaboración: los autores

F) Evaluación de riesgos del proyecto

Riesgos generales

Probabilidad	Valor numérico	Impacto	Valor numérico	Tipo de riesgo	Probabilidad x Impacto
Muy improbable	1	Muy bajo	1	Muy alto	Mayor a 49
Relativamente probable	2	Bajo	2	Alto	30 - 49
Probable	3	Moderado	3	Moderado	20 - 29
Muy probable	4	Alto	4	Bajo	10 - 19
Casi certeza	5	Muy alto	5	Muy bajo	Menor a 10

Descripción del riesgo	Causa raíz	Trigger	Probabilidad	Objetivo afectado	Estimación de impacto	Prob. x Impacto	Tipo de riesgo
Incumplimiento de las actividades del cronograma del proyecto	Poca disponibilidad de tiempo de los recursos	Recarga de los recursos en otras actividades / Proyectos	5	*Alcance*	1	5	**Alto**
				Tiempo	5	25	
				Costo	1	5	
				Calidad	2	10	
				Total Probabilidad x Impacto		**45**	
Cambios en las prioridades	Decisión de gerencia	Surgimiento de actividades más importantes	3	*Alcance*	3	9	**Alto**
				Tiempo	5	15	
				Costo	2	6	
				Calidad	2	6	
				Total Probabilidad x Impacto		**36**	

Descripción del riesgo	Causa raíz	Trigger	Estimación de probabilidad	Objetivo afectado	Estimación de impacto	Prob. x Impacto	Tipo de riesgo
Trabajos no programados	Solicitud del Comité del SGSI	Falla en la planificación de actividades	3	*Alcance*	2	6	**Alto**
				Tiempo	5	15	
				Costo	2	6	
				Calidad	3	9	
				Total Probabilidad x Impacto		**36**	
Cambios en el alcance del proyecto	Decisión de gerencia	Surgimiento de nuevas necesidades de la Gerencia	2	*Alcance*	5	10	**Moderado**
				Tiempo	5	10	
				Costo	2	4	
				Calidad	2	4	
				Total Probabilidad x Impacto		**28**	
Modificación del cronograma del Proyecto	Solicitud del Comité del SGSI.	Conversaciones o consultas informales	3	*Alcance*	1	3	**Moderado**
				Tiempo	3	9	
				Costo	2	6	
				Calidad	2	6	
				Total Probabilidad x Impacto		**24**	
Falta temporal de Personal clave	Vacaciones, enfermedad, permisos, entre otros.	---	3	*Alcance*	1	3	**Moderado**
				Tiempo	3	9	
				Costo	2	6	
				Calidad	2	6	
				Total Probabilidad x Impacto		**24**	

Descripción del riesgo	Causa raíz	Trigger	Estimación de probabilidad	Objetivo afectado	Estimación de impacto	Prob. x Impacto	Tipo de riesgo
Pérdida de personal clave	Término de contrato, despido, renuncia, etc.	---	1	*Alcance*	1	4	**Bajo**
				Tiempo	3	3	
				Costo	2	2	
				Calidad	2	4	
				Total Probabilidad x Impacto		**13**	
Restructuración Institucional	Cambio en la estructura organizacional de la gerencia	Disconformidad con la estructura actual	1	*Alcance*	4	4	**Bajo**
				Tiempo	4	4	
				Costo	2	2	
				Calidad	2	2	
				Total Probabilidad x Impacto		**12**	

Cuadro 3.9: Evaluación de riesgos del proyecto [38]

Riesgos específicos

Probabilidad	Valor numérico	Impacto	Valor numérico	Tipo de riesgo	Probabilidad x Impacto
Muy Improbable	1	Muy Bajo	1	Muy Alto	Mayor a 49
Relativamente Probable	2	Bajo	2	Alto	30 - 49
Probable	3	Moderado	3	Moderado	20 - 29
Muy Probable	4	Alto	4	Bajo	10 - 19
Casi Certeza	5	Muy Alto	5	Muy Bajo	Menor a 10

[38] Elaboración: los autores

Riesgos	Descripción del riesgo	Estimación de probabilidad	Objetivo afectado	Estimación de impacto	Prob. x Impacto	Tipo de riesgo
RE1	**Procesos de Tecnología definidos incorrectamente**	4	*Alcance*	5	20	**Muy Alto**
			Tiempo	3	12	
			Costo	1	4	
			Calidad	5	20	
			Total Probabilidad por Impacto		**56**	
RE2	**Desconocimiento del Equipo Implementador para la elaboración del Plan de Continuidad**	4	*Alcance*	3	12	**Alto**
			Tiempo	3	12	
			Costo	1	4	
			Calidad	3	12	
			Total Probabilidad por Impacto		**40**	
RE3	**Incorrecta definición de activos de información de los procesos**	3	*Alcance*	2	6	**Alto**
			Tiempo	5	15	
			Costo	1	3	
			Calidad	5	15	
			Total Probabilidad por Impacto		**39**	
RE4	**Incorrecta Identificación de los riesgos en los Activos de Información**	3	*Alcance*	2	6	**Alto**
			Tiempo	5	15	
			Costo	1	3	
			Calidad	5	15	
			Total Probabilidad por Impacto		**39**	

Riesgos	Descripción del riesgo	Estimación de probabilidad	Objetivo afectado	Estimación de impacto	Prob. x Impacto	Tipo de riesgo
RE5	**Incorrecta definición de controles para los riesgos**	3	*Alcance*	2	6	**Alto**
			Tiempo	5	15	
			Costo	2	6	
			Calidad	4	12	
			Total Probabilidad por Impacto		**39**	
RE6	**El Equipo Implementador SGSI no se encuentra comprometido con el proyecto**	3	*Alcance*	1	3	**Alto**
			Tiempo	5	15	
			Costo	1	3	
			Calidad	5	15	
			Total Probabilidad por Impacto		**36**	
RE7	**Personal de Tecnologías no se encuentra capacitado para la implementación de un SGSI**	3	*Alcance*	1	3	**Alto**
			Tiempo	5	15	
			Costo	1	3	
			Calidad	5	15	
			Total Probabilidad por Impacto		**36**	
RE8	**Desconocimiento del Equipo Implementador sobre las entidades externas que afectan a los procesos**	3	*Alcance*	2	6	**Moderado**
			Tiempo	3	9	
			Costo	1	3	
			Calidad	3	9	
			Total Probabilidad por Impacto		**27**	

Riesgos	Descripción del riesgo	Estimación de probabilidad	Objetivo afectado	Estimación de impacto	Prob. x Impacto	Tipo de riesgo
RE9	**Personal de Tecnología no cumple con los controles definidos en la Implementación.**	3	*Alcance*	1	3	**Moderado**
			Tiempo	1	3	
			Costo	2	6	
			Calidad	5	15	
			Total Probabilidad por Impacto		**27**	
RE10	**Elaboración del Plan de Tratamiento de Riesgos con fechas equivocadas.**	2	*Alcance*	1	2	**Moderado**
			Tiempo	5	10	
			Costo	1	2	
			Calidad	5	10	
			Total Probabilidad por Impacto		**24**	
RE11	**Demora en Aprobación de políticas, manuales, procedimientos, instructivos y otros documentos relacionados al SGSI**	3	*Alcance*	1	3	**Moderado**
			Tiempo	5	15	
			Costo	1	3	
			Calidad	1	3	
			Total Probabilidad por Impacto		**24**	
RE12	**Formatos inadecuados para el análisis y Evaluación de riesgos**	2	*Alcance*	1	2	**Moderado**
			Tiempo	4	8	
			Costo	1	2	
			Calidad	5	10	
			Total Probabilidad por Impacto		**22**	

Riesgos	Descripción del riesgo	Estimación de probabilidad	Objetivo afectado	Estimación de impacto	Prob. x Impacto	Tipo de riesgo
RE13	**El Comité SGSI no se encuentra comprometido con el proyecto**	2	*Alcance*	1	2	Bajo
			Tiempo	2	4	
			Costo	1	2	
			Calidad	5	10	
			Total Probabilidad por Impacto		**18**	
RE14	**Incumplimiento de los Programa y Planes de Auditorías Internas**	2	*Alcance*	1	2	Bajo
			Tiempo	3	6	
			Costo	2	4	
			Calidad	3	6	
			Total Probabilidad por Impacto		**18**	

Cuadro 3.10: Riesgos específicos del proyecto [39]

[39] Fuente. Elaboración por los autores.

G) Respuesta de riesgos del proyecto

Riesgos generales

Riesgos	Responsable de tratamiento	Plan de mitigación		Plan de contingencia
RG1	-Jefe de Centro de Cómputo - Jefe de Desarrollo - Coordinador B.I.	- Aprobación del cronograma por la Gerencia de Tecnología, previa revisión por los involucrados.		- Liberar a los recursos de actividades no relacionadas con el proyecto. - Personal de apoyo para los recursos responsables de actividades del proyecto.
RG2	Facilitador SGSI	- Aprobación del cronograma por la Gerencia de Tecnología, previa revisión por los involucrados.		- Rápida adaptación del cronograma del proyecto. - Concientización de los involucrados.
RG3	Facilitador SGSI	- Aprobación del cronograma por la Gerencia de Tecnología, previa revisión por los involucrados.		- Rápida adaptación del cronograma del proyecto. - Asignación de recursos a los nuevos trabajos.
RG4	Facilitador SGSI	- Revisión y aprobación del Alcance del SGSI por la Gerencia de Tecnología y Gerencias afectadas.		- Reunión con la gerencia. - Adaptación del alcance, política y cronograma. - Ajustes en los recursos sujetos al nuevo alcance (en caso requiera).
RG5	Facilitador SGSI	- Aprobación del cronograma por la Gerencia de Tecnología, previa revisión por los involucrados.		- Rápida adaptación del cronograma del proyecto, previa coordinación con los involucrados.

Riesgos	Responsable de tratamiento	Plan de mitigación	Plan de contingencia
RG6	Gerente de Tecnología	- Revisión del cronograma de vacaciones. - Realizar ajustes el Cronograma y aprobarlo por Gerencia de Tecnología.	- Sustitución temporal del personal por un perfil similar.
RG7	---	---	---
RG8	---	---	---

Cuadro 3.11: Respuesta a riesgos del proyecto [40]

Riesgos específicos

Riesgos	Responsable de tratamiento	Plan de mitigación	Plan de contingencia
RE1	- Jefe Centro de Cómputo - Jefe de Desarrollo - Coordinador BI	- El jefe de cada Dpto. debe reunirse con el personal a cargo para la definición de todos los procesos ejecutados.	- El jefe de cada Dpto. debe solicitar apoyo al Dpto. de Gestión de Procesos para re-definir los procesos.

[40] Elaboración: los autores

RE2	Jefe Centro de Cómputo	- Capacitación en la elaboración de un Plan de Continuidad de Tecnología.		- Sub Contratar a un tercero para elaborar el Plan de Continuidad - Sub Contratar una Capacitación externa
Riesgos	**Responsable de tratamiento**	**Plan de mitigación**		**Plan de contingencia**
RE3	- Jefe Centro de Cómputo - Facilitador SGSI	- Realizar presentaciones con metodología para la identificación de activos.		- Participar de reuniones con los responsables para la definición de los activos de información a cargo.
RE4	- Jefe Centro de Cómputo - Facilitador SGSI	- Realizar presentaciones con metodología para la identificación de riesgos.		- Participar de reuniones con los responsables para la identificación de los activos de los riesgos.
RE5	- Jefe Centro de Cómputo - Facilitador SGSI	- Realizar presentaciones con metodología para la definición de controles aplicables. - Facilitar un formato con todos los controles aplicables		- Participar de reuniones con los responsables para la definición de los controles aplicables.
RE6	- Jefe Centro de Cómputo - Facilitador SGSI	- Realizar presentación de concientización al Equipo Implementador.		- Coordinar reunión con la Gerencia de Tecnología para revisar avance de proyecto.

RE7	- Jefe Centro de Cómputo - Facilitador SGSI	- Capacitar al personal de los Dptos. Involucrados para la implementar el Plan de Tratamiento de Riesgos.		- Sub Contratar a un tercero para elaborar el Plan de Continuidad - Sub Contratar una Capacitación externa
RE8	- Jefe Centro de Cómputo - Jefe de Desarrollo - Coordinador BI	- Elaborar una lista con todas las entidades externas con las cuales se ejecutan los procesos.		- Revisar los procesos definidos y las entidades externas que los afectan. - Actualizar listado de entidades externas.
Riesgos	**Responsable de tratamiento**	**Plan de mitigación**		**Plan de contingencia**
RE9	- Jefe Centro de Cómputo - Facilitador SGSI	- Capacitar al personal de los Dptos. Involucrados para la cumplir con los controles definidos.		- Coordinar reunión con la Gerencia de Tecnología y Jefaturas responsables para revisar avance de proyecto.
RE10	- Jefe Centro de Cómputo - Facilitador SGSI	- Aprobación del Plan de Tratamiento de Riesgos por la Gerencia de Tecnología, previa revisión por los involucrados.		- Rápida adaptación del nuevo Plan de Tratamiento de Riesgos. - Concientización de los involucrados.
RE11	- Jefe Centro de Cómputo - Facilitador SGSI	- Definir método con tiempos para la revisión y aprobación de documentos.		- Enviar un correo a involucrados con copia a Gerencia de Tecnología, informando publicación de algún documento del SGSI.
RE12	- Jefe Centro de Cómputo - Facilitador SGSI	- Aprobación y revisión de todos los formatos a usar, por las Jefaturas y Gerencia.		- Re definir los formatos en reunión con el Comité del SGSI. - Actualizar cronograma de implementación.

RE13	---	---		---
RE14	---	---		---

Cuadro 3.12: Respuesta a riesgos específicos del proyecto [41]

[41] Elaboración: los autores

3.2.1.3 Ejecución del proyecto

A) Matriz de selección de proveedores

Nº	CRITERIOS INDIVIDUALES	FACTOR	COSAPI DATA		JAPAN COMPUTER		IBM		ACCESOR		SISBIOCOL CO	
			Calificación	%	Calificación	%	Calificación	%	Calificación	%	Calificación	%
1	Forma de Pago	**3**	9	27%	8	24%	8	24%		0%	10	30%
2	Escala de Precios	**3**	8	24%	5	15%	4	12%	7	21%	8	24%
3	Ofrece/Cumple servicio post venta y/o servicio técnico	**10**	8	80%	7	70%	9	90%	8	80%	9	90%
4	Ofrece/Cumple garantía de producto / servicio	**10**	10	100%	8	80%	9	90%	9	90%	9	90%
5	Verificación de que las muestras del producto cumplan con las especificaciones requeridas.	**3**	9	27%	9	27%	10	30%	8	24%	9	27%
6	Cumple con disponibilidad inmediata y stock de productos	**5**	9	45%	8	40%	9	45%	9	45%	10	50%
7	Cumple con entregar el producto o servicio de acuerdo a las especificaciones técnicas.	**7**	10	70%	8	56%	10	70%	8	56%	9	63%
8	Cumple con entregar las cantidades de productos o servicios.	**7**	10	70%	7	49%	9	63%	10	70%	10	70%
9	Cumple con el tiempo de entrega del producto o servicio.	**7**	10	70%	8	56%	9	63%	7	49%	9	63%
TOTAL			**57%**		**46%**		**54%**		**48%**		**56%**	
CLASIFICACIÓN DEL RESULTADO			**SI**		**NO**		**SI - NO**		**NO**		**SI**	

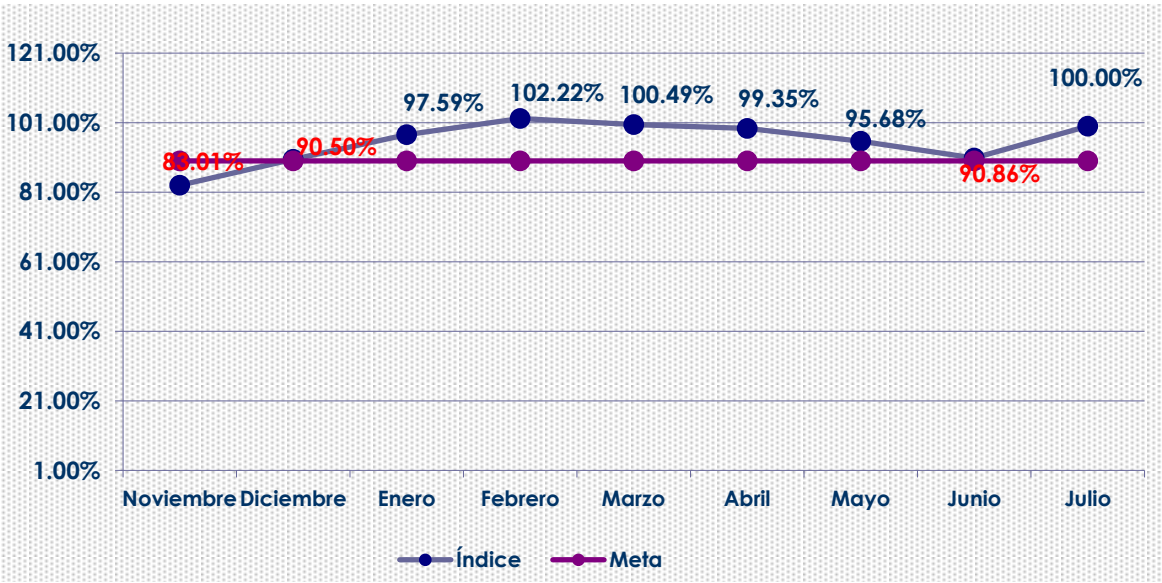
Cuadro 3.12: Matriz de selección de proveedores [42]

[42] Elaboración: los autores

3.2.1.4 Seguimiento y control

A) Seguimiento mensual del proyecto

Mes	Avance Real	Avance Esperado	Índice
Noviembre	15.00%	18.07%	83.01%
Diciembre	27.15%	30.00%	90.50%
Enero	53.25%	54.57%	97.59%
Febrero	60.00%	58.70%	102.22%
Marzo	69.54%	69.20%	100.49%
Abril	75.00%	75.49%	99.35%
Mayo	78.00%	81.52%	95.68%
Junio	80.00%	88.04%	90.86%
Julio	100.00%	100.00%	100.00%



Cuadro 3.13: Seguimiento mensual de proveedores [43]

[43] Elaboración: los autores

B) Control de cambios

Nro.	Tipo	Situación actual	Descripción	Actividad afectada	Impacto en el cronograma	Fecha de cambio
1	Preventivo	No se cuenta con el Manual del SGSI	Se cambió el **Alcance SGSI**, por el Manual SGSI (Contiene el alcance en el punto 7.1.2.1.A)	1.1.2	Ninguno	10-ene
2	Preventivo	No se cuenta con Formato para inventariar los activos de información	Se modificó las actividades de Formatos SGSI. Se agregó el formato **Inventario de Activos** y Plan de Tratamiento de Riesgos	1.5.1.5	Ninguno	16-ene
3	Preventivo	No se consideró el Inventario de activos de información	Se agregó la actividad: Elaborar **Inventario de activos de información**	1.5.2.3 1.5.3.3 1.5.4.3	Ninguno	25-ene
4	Preventivo	No se cuenta con un manual de la metodología de Análisis y Gestión de Riesgos de A.I.	Se incluyó el Manual de la Metodología de Análisis y Gestión de Riesgos para que sirva como base de conocimientos para proyectos futuros.	1.5.2.1	Ninguno	14-mar
5	Correctivo	Exceso de tiempo en revisión de Riesgos y Controles de Mitigación por parte de la Gerencia.	Incremento de dos semanas en la Planificación de Controles. Se desplazó la implementación de controles en una semana.	3.2	Ninguno	07-Abr

Cuadro 3.14: Control de cambios [44]

3.2.1.5 Cierre

A) Acta de cierre del proyecto

Hoy 22 de junio del 2012, siendo las 05:00 P.M., se procede al cierre del Proyecto de “Diseño e Implementación del Sistema de Gestión de Seguridad de Información” en los procesos de Tecnología de la empresa Card Perú S.A.

Declaración formal de la aceptación del proyecto:

Por parte de la presente se deja constancia que el Proyecto a cargo de “Carlos Barrantes y Javier Hugo”, ha sido aceptado y aprobado por la Gerencia de Tecnología de la empresa Card Perú S.A., dando constancia por la presente que el proyecto ha culminado exitosamente.

[44] Elaboración: los autores

3.2.2 Diseño e Implementación del SGSI

3.2.2.1 Política SGSI

Card Perú S.A. es una empresa dedicada a la “Emisión y administración de tarjetas de crédito y servicios financieros”. Conscientes de la importancia que la seguridad de la información tiene para el desarrollo del negocio, se ha decidido implantar un Sistema de Gestión de Seguridad de Información **(SGSI)**, que se suscribe en la presente política.

- El Comité del SGSI define y revisa los objetivos del SGSI, enfocados a la conservación de la **confidencialidad**, **disponibilidad** e **integridad** de los activos de información, considerados como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios. Cumpliendo todos los requisitos legales, reglamentarios y contractuales que le sean de aplicación, que incrementa de esta manera, la confianza de nuestros clientes, accionistas y otras partes interesadas.

- El diseño, implantación y mantenimiento del SGSI se apoya en los resultados de un proceso continuo de análisis y gestión de riesgos, del que se derivan las acciones a desarrollar en materia de seguridad dentro del Alcance del SGSI (**Ve**r **3.2.2.2 manual del SGSI**).

- El comité del SGSI establece los criterios de evaluación del riesgo de manera que todos aquellos escenarios que impliquen un nivel de riesgo inaceptable sean tratados adecuadamente.

- Se debe implantar las medidas requeridas para la formación y concientización del personal en seguridad de la información. Asimismo, en caso que los trabajadores incumplan las políticas de seguridad, la dirección podrá ejecutar las medidas disciplinarias que se encuentren dentro del marco legal aplicable.

- La gerencia de tecnología se compromete con la implantación, mantenimiento y mejora del SGSI facilitando los medios y recursos que sean necesarios.

- Es responsabilidad del oficial de seguridad de Información asegurar el buen funcionamiento del SGSI.

- La presente política es de aplicación a todo el personal y recursos que se encuentran dentro del Alcance del SGSI **(Ve**r **3.2.2.2 manual del SGSI**). Se pone en su conocimiento y es comunicada a todas las partes interesadas.

3.2.2.2 Manual

A) Objetivo

El objetivo del presente manual es proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de seguridad de información de la gerencia de tecnología de Card Perú S.A.

B) Alcance

Aplica a todos los procesos ejecutados en los departamentos de centro de cómputo, business intelligence y desarrollo de la gerencia de tecnología.

C) Responsabilidad

La gerencia de tecnología es responsable de la aplicación efectiva del presente manual, jefe de centro de cómputo, jefe de desarrollo y coordinador de business intelligence de su correcta ejecución.

D) Definiciones

- **Activo :** Todo aquel medio y/o recurso que maneja información de valor para la organización.
- **Equipo SGSI :** Equipo multidisciplinario del apoyo a la gerencia de tecnología para la implementación del SGSI.
- **Disponibilidad :** La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- **Confidencialidad :** La propiedad que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.
- **Integridad :** Propiedad de salvaguardar la exactitud e integridad de los activos.

- **Seguridad de información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Riesgo residual :** Es el riesgo remanente después del tratamiento del riesgo.
- **Análisis del riesgo :** Uso sistemático de la información para identificar fuentes y para estimar el riesgo.
- **Evaluación del riesgo :** Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.
- **Gestión del riesgo :** Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
- **Tratamiento del riesgo :** Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.
- **No conformidad :** Incumplimiento de un requisito normativo, contractual y/o legal.

E) Símbolos y abreviaturas

- **SGSI :** Sistema de gestión de seguridad de información.
- **SBS :** Superintendencia de banca y seguros

F) Descripción

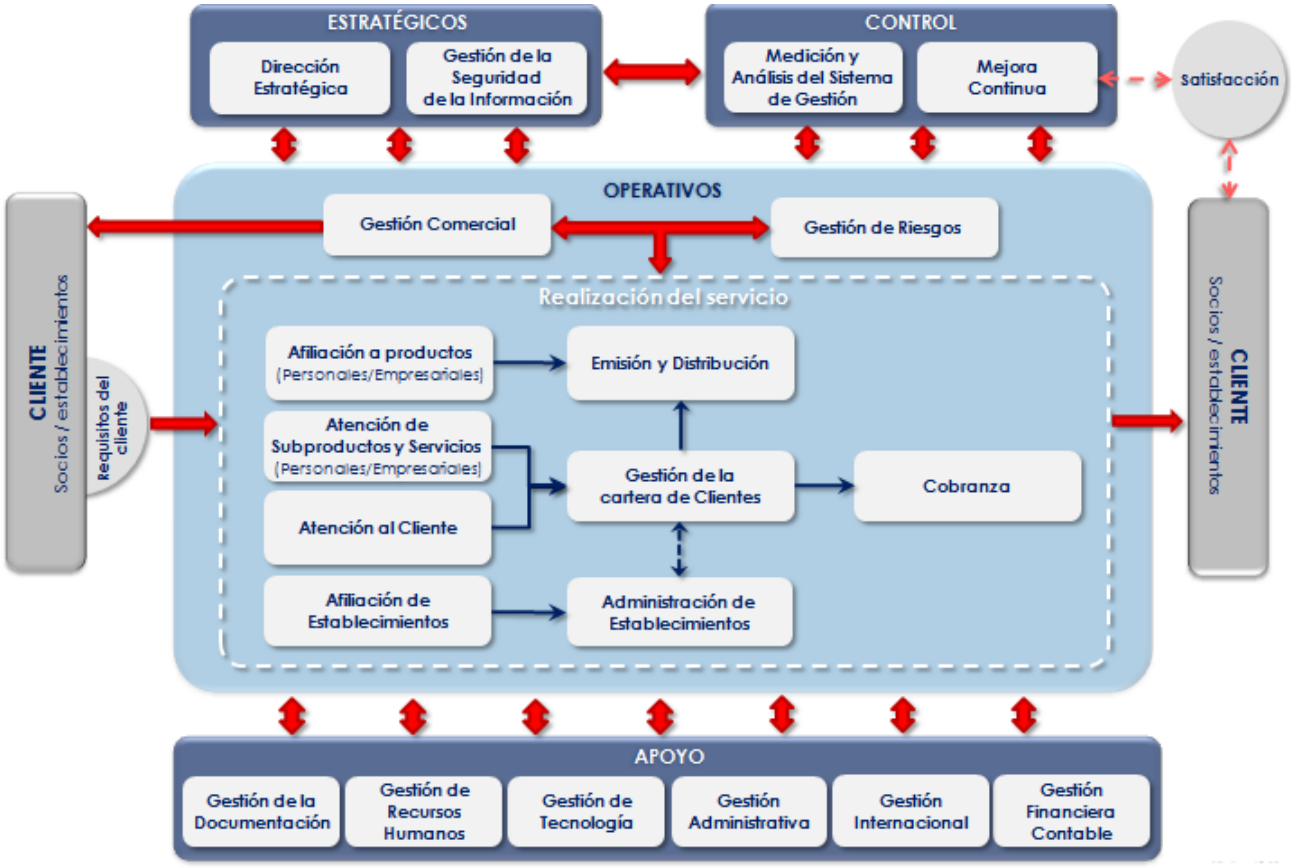
- **Requerimientos generales**

La gerencia de tecnología establece, implementa, opera, monitorea, mantiene y mejora continuamente el SGSI documentado dentro del contexto de las actividades comerciales generales de Card Perú S.A. y los riesgos que enfrentan.

- **Establecimiento y manejo del SGSI**
  - **Establecimiento del SGSI**

a) Descripción del alcance

La Gerencia de Tecnología define el alcance y los límites del SGSI en términos de las características de Card Perú S.A, que cuenta actualmente con los procesos de negocio: [45]



El sistema de gestión de la seguridad de la información aplica en todos los procesos que se ejecutan bajo la Gerencia de tecnología.

b) Política del SGSI

De acuerdo con el **artículo 3° (a) G-140**, la Gerencia de Tecnología define la **política SGSI (Ver 3.2.2.1)** en términos de las características Card Perú S.A., que:

- Incluye el marco referencial para establecer los objetivos.
- Toma en cuenta los requerimientos comerciales, legales, reguladores, y las obligaciones de la seguridad contractual.

[45] Elaboración: los autores

- Está alineada con el contexto de la gestión del riesgo estratégico de la gerencia de tecnología en el cual se da el establecimiento y mantenimiento del SGSI.
- Establece el criterio con el que se evalúa el riesgo,
- Ha sido revisada y aprobada por la gerencia.

c) Identificación de los riesgos

De acuerdo al **Artículo 3° (b) G-140**, la Gerencia de Tecnología:

- Identifica los activos según punto **3.1.3.2.4.B identificación de activos de seguridad de información** dentro del alcance del SGSI.
- Identifica las amenazas para aquellos activos.
- Identifica las vulnerabilidades que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos, según el **punto 3.1.3.2.4.D análisis y evaluación de riesgos.**

d) Análisis y evaluación de riesgos

De acuerdo al **artículo 3° (b) G-140**, la gerencia de tecnología:

- Calcula el impacto comercial sobre Card Perú S.A. que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos,
- Calcula la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, los impactos asociados con estos activos, y los controles implementados actualmente,
- Calcula los niveles de riesgo,

- Determina si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo, según el **punto 3.1.3.2.4.D Análisis y evaluación de riesgos.**

e) Gestión y tratamiento de riesgos

De acuerdo al **artículo 3° (b) G-140,** la Gerencia de Tecnología realiza acciones según el **punto 3.1.3.2.5 determinación del riesgo,** que incluyen:

- Aplicar los controles apropiados.
- Aceptar los riesgos de forma consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo de Card Perú S.A.
- Evitar los riesgos.
- Transferir los riesgos a otras entidades.

- **Implementación y operación del SGSI**

  La Gerencia de Tecnología:

  - Formula el **tratamientos de riesgos** que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.
  - De acuerdo al **artículo 4° (b) G-140**, la Gerencia de Tecnología coordina, monitorea e implementa el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales tienen en consideración el financiamiento y asignación de roles y responsabilidades.
  - De acuerdo al **artículo 5° G-140**, Implementa todos los controles seleccionados que satisfacen los objetivos del SGSI, dentro de la seguridad lógica, seguridad de personal, seguridad física/ambiental, inventariado de

activos y clasificación de información, administración de las operaciones y comunicaciones, adquisición, desarrollo y mantenimiento de sistemas, procedimientos de respaldo, gestión de incidentes de seguridad de información, cumplimiento normativo y privacidad de la información.

- Define cómo medir la efectividad de los controles o grupos de controles seleccionados y especifica cómo se van a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles.

- **Monitoreo y revisión del SGSI**

  - La Gerencia de Tecnología ejecuta controles de monitoreo y revisión, para:
    - Detectar prontamente los errores en los resultados de procesamiento.
    - De acuerdo al **artículo 4° (d) G-140**, Identifica y evalúa los incidentes y violaciones de seguridad fallidas y exitosas, para tomar acciones apropiadas.
    - Ayudar a detectar eventos de seguridad, evitando así los incidentes de seguridad, mediante el uso de indicadores.
    - Determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

  - La Gerencia de Tecnología realiza revisiones regulares de la efectividad del SGSI tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.

- La Gerencia de Tecnología mide la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

- La Gerencia de Tecnología revisa las evaluaciones del riesgo a intervalos planeados y revisa el nivel del riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:
  - Card Perú S.A.
  - La misma gerencia de tecnología
  - Objetivos y procesos comerciales
  - Amenazas identificadas
  - Efectividad de los controles implementados
  - Eventos externos como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social

- La Gerencia de Tecnología realiza auditorías internas al SGSI a intervalos planificados.

- **Mantener y mejorar el SGSI**

  - La gerencia de tecnología:
    - Implementa las mejoras identificadas en el SGSI,
    - Toma las acciones correctivas y preventivas apropiadas,
    - Comunica los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo con las circunstancias y, cuando sea relevante, acuerda como proceder,
    - Asegura que las mejoras logren sus objetivos señalados.

- **Requerimientos de la documentación**

  La documentación del SGSI incluye lo siguiente:

- De acuerdo al **artículo 3° (a) G-140,** la **política SGSI (ver 3.2.2.1)** y los objetivos,
- El alcance del SGSI,
- De acuerdo al **artículo 5° G-140**, procedimientos y controles de soporte del SGSI,
- De acuerdo al **artículo 3° (b) G-140,** la metodología de la evaluación de riesgos,
- Los procedimientos documentaos necesarios para la Gerencia de Tecnología para asegurar la planeación, operación y control e sus procesos de seguridad de información,
- De acuerdo al **artículo 3° (c) G-140,** los registros requeridos por la SBS,

- **Control de documentos**

Los documentos requeridos por el SGSI son protegidos y controlados, para los cuales se siguen los siguientes lineamientos:

- Aprobar la idoneidad de los documentos antes de su emisión.
- Revisar y actualizar los documentos conforme sea necesario y re-aprobar los documentos.
- Asegurar que se identifiquen los cambios y el estado de la revisión actual de los documentos.
- Asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso.
- Asegurar que los documentos se mantengan legibles y fácilmente identificables.
- Asegurar que los documentos estén disponibles para aquellos que los necesitan; y sean transferidos, almacenados y finalmente eliminados.
- Asegurar que se identifiquen los documentos de origen externo,
- Asegurar que se controle la distribución de los documentos,
- Evitar el uso indebido de documentos obsoletos,

- Aplicarles una identificación adecuada si se van a retener por algún motivo.

- **Control de registros**

De acuerdo al **artículo 3° (c) G-140**, la Gerencia de Tecnología establece y mantiene registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI son protegidos y controlados.

El SGSI toma en cuenta cualquier requerimiento legal o regulador relevante. Los registros se mantienen legibles, fácilmente identificables y recuperables. Se mantienen documentados e implementados los controles necesarios para la identifican, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros.

- **Responsabilidad de la gerencia**
  - **Provisión de recursos:** La gerencia de tecnología determina y proporciona los recursos necesarios para:
    - Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI,
    - Asegurar que los procedimientos de seguridad de la información respalden los requerimientos comerciales,
    - Identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales,
    - Mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados,
    - Llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones.
  - **Capacitación, conocimiento y capacidad:** De acuerdo al **artículo 4° (c)**, la gerencia de tecnología se asegura que todo el personal a quien se le asignó responsabilidades definidas en el

SGSI sea competente para realizar las tareas requeridas, para lo cual se:

- Determina las capacidades necesarias para el personal que realiza trabajo que afecta al SGSI,
- Proporciona la capacitación,
- Evaluar la efectividad de las acciones tomadas,
- Mantienen registros de educación, capacitación, capacidades, experiencia y calificaciones.

➢ **Revisión gerencial del SGSI**

La Gerencia de Tecnología revisa el SGSI para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión incluye oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información.

➢ **Mejoramiento del SGSI**

- **Mejora continua:** La Gerencia de Tecnología mejora continuamente la efectividad del SGSI a través del uso de la **política SGSI**, objetivos de seguridad de la información, resultados de auditoría, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.
- **Acciones correctivas:** La Gerencia de Tecnología realiza las acciones necesarias para eliminar las causas de las no conformidades con los requerimientos del SGSI para poder evitar la recurrencia, para lo cual se deben realizar las siguientes actividades:

  - Identificar las no conformidades.
  - Determinar las causas de las no conformidades.
  - Evaluar la necesidad de acciones para asegurar que las no conformidades no vuelvan a ocurrir.
  - Determinar e implementar la acción correctica necesaria,

- Registrar los resultados de la acción tomada.

- **Acciones preventivas:** La gerencia de tecnología realiza las acciones necesarias para eliminar las causas de las no conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia para lo cual se deben realizar las siguientes actividades:

  - Identificar las no conformidades potenciales y sus causas.
  - Evaluar la necesidad para la acción para evitar la ocurrencia de no conformidades.
  - Determinar e implementar la acción preventiva necesaria.
  - Registrar los resultados de la acción tomada.
  - Revisar la acción preventiva tomada.

3.2.2.3 Análisis de brechas PRE

Ítem	Requisitos Circular G-140	Cumple	Nivel cumplimiento	
Generalidades				
1	Definición y difusión de una política	**SÍ**	50%	
2	Metodología de Gestión de Riesgos	**SÍ**	80%	
3	Mantenimiento de Registros	**SÍ**	50%	
4	Estructura organizacional definida y difundida	**SÍ**	50%	
5	Asegurar el cumplimiento de la política	**NO**	0%	**29%**
6	Monitoreo de la implementación de controles	**NO**	0%	
7	Método para la concientización y entrenamiento del personal	**NO**	0%	
8	Método para la evaluación de incidentes de seguridad / acciones	**NO**	0%	
Seguridad lógica				
9	Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.	**SÍ**	50%	
10	Revisiones periódicas sobre los derechos concedidos a los usuarios.	**SÍ**	50%	
11	Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.	**SÍ**	100%	**42%**
12	Controles especiales sobre utilidades del sistema y herramientas de auditoría.	**NO**	0%	
13	Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.	**NO**	0%	
14	Controles especiales sobre usuarios remotos y computación móvil.	**SÍ**	50%	

Cuadro 3.15: Análisis de brechas PRE [46]

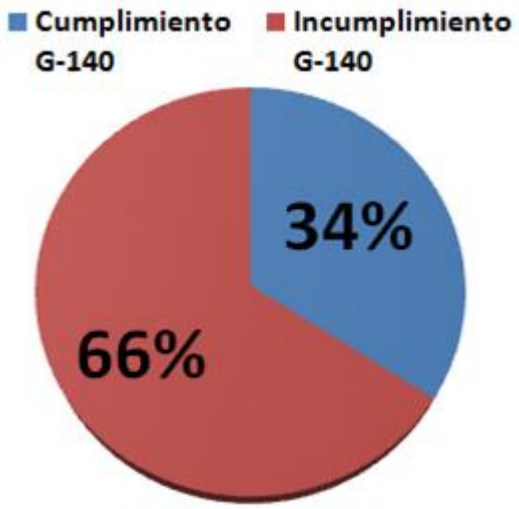
[46] Elaboración: los autores

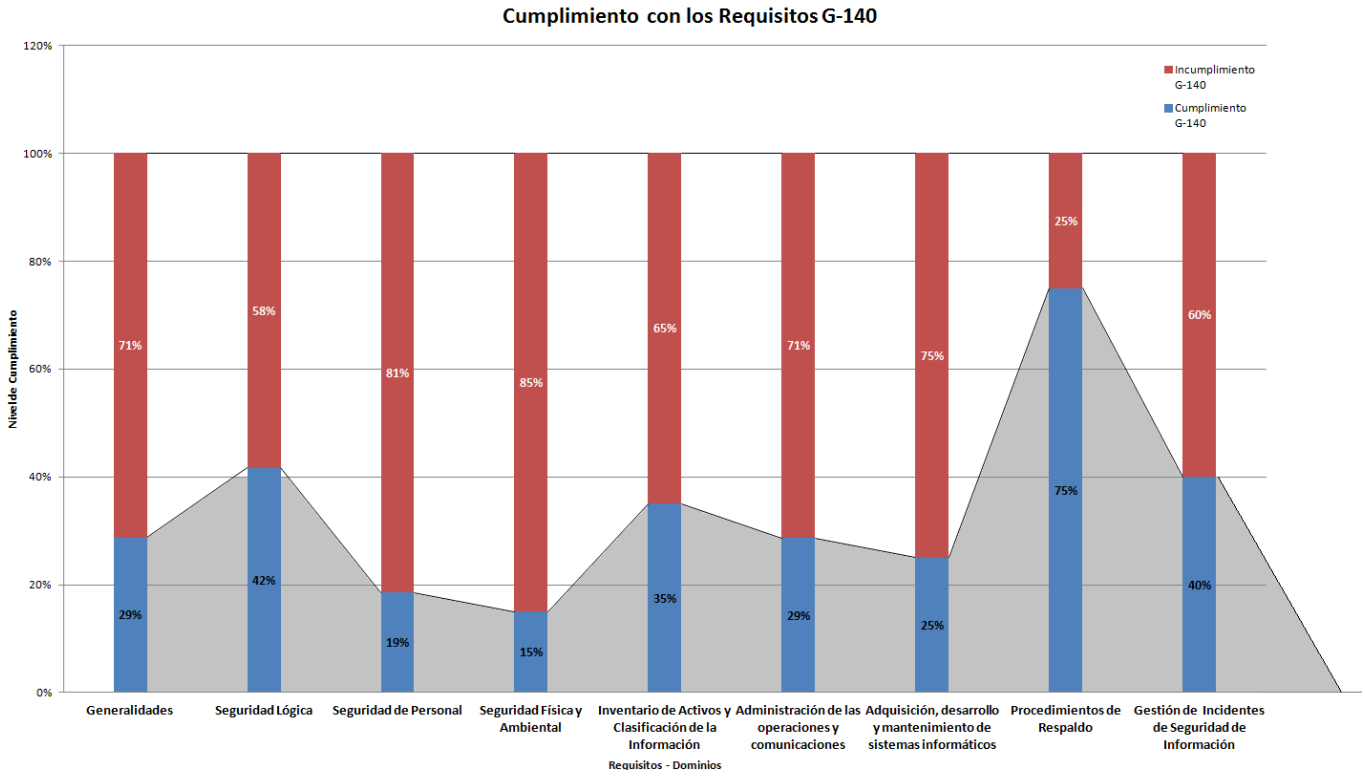
Ítem	Requisitos Circular G-140	Cumple	Nivel Cumplimiento	
Seguridad de personal				
15	Definición de roles y responsabilidades establecidos sobre la seguridad de información.	**NO**	0%	**19%**
16	Verificación de antecedentes, de conformidad con la legislación laboral vigente.	**SÍ**	100%	
17	Concientización y entrenamiento.	**NO**	0%	
18	Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.	**NO**	0%	
19	Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.	**NO**	0%	
Seguridad física y ambiental				
20	Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.	**SÍ**	15%	**15%**
21	Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.	**SÍ**	15%	
Inventario de activos y clasificación de la información				
22	Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.	**SÍ**	50%	**35%**
23	Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.	**SÍ**	20%	

Ítem	Requisitos Circular G-140	Cumple	Nivel cumplimiento	
Administración de las operaciones y comunicaciones				
24	Procedimientos documentados para la operación de los sistemas.	**SÍ**	10%	
25	Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.	**NO**	0%	
26	Separación de funciones para reducir el riesgo de error o fraude.	**NO**	0%	
27	Separación de los ambientes de desarrollo, pruebas y producción.	**SÍ**	50%	
28	Monitoreo del servicio dado por terceras partes.	**SÍ**	50%	
29	Administración de la capacidad de procesamiento.	**NO**	0%	**29%**
30	Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.	**SÍ**	100%	
31	Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.	**SÍ**	30%	
32	Seguridad sobre el intercambio de la información, incluido el correo electrónico.	**SÍ**	25%	
33	Seguridad sobre canales electrónicos.	**SÍ**	50%	
34	Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.	**NO**	0%	

ÍTEM	Requisitos Circular G-140	Cumple	Nivel cumplimiento	
Adquisición, desarrollo y mantenimiento de sistemas informáticos				
35	Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.	**NO**	0%	**25%**
36	Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.	**NO**	0%	
37	Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.	**SÍ**	50%	
38	Controlar el acceso a las librerías de programas fuente.	**NO**	50%	
39	Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.	**SÍ**	50%	
40	Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.	**NO**	0%	
Procedimientos de respaldo				
41	Procedimientos de respaldo regular y periódicamente validado. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la empresa.	**SÍ**	50%	**75%**
42	Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento.	**SÍ**	100%	

Gestión de incidentes de seguridad de información				
43	Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.	NO	0%	40%
44	Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.	SÍ	80%	

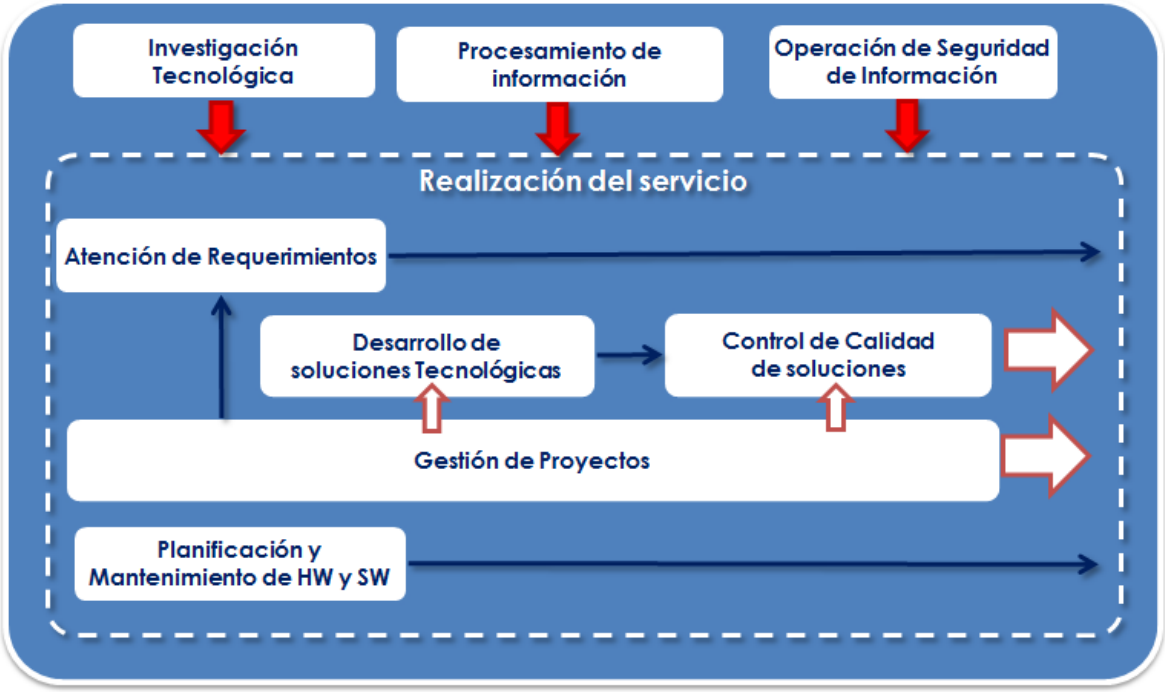




3.2.2.4 Análisis y evaluación de riesgos

A) Identificación de procesos

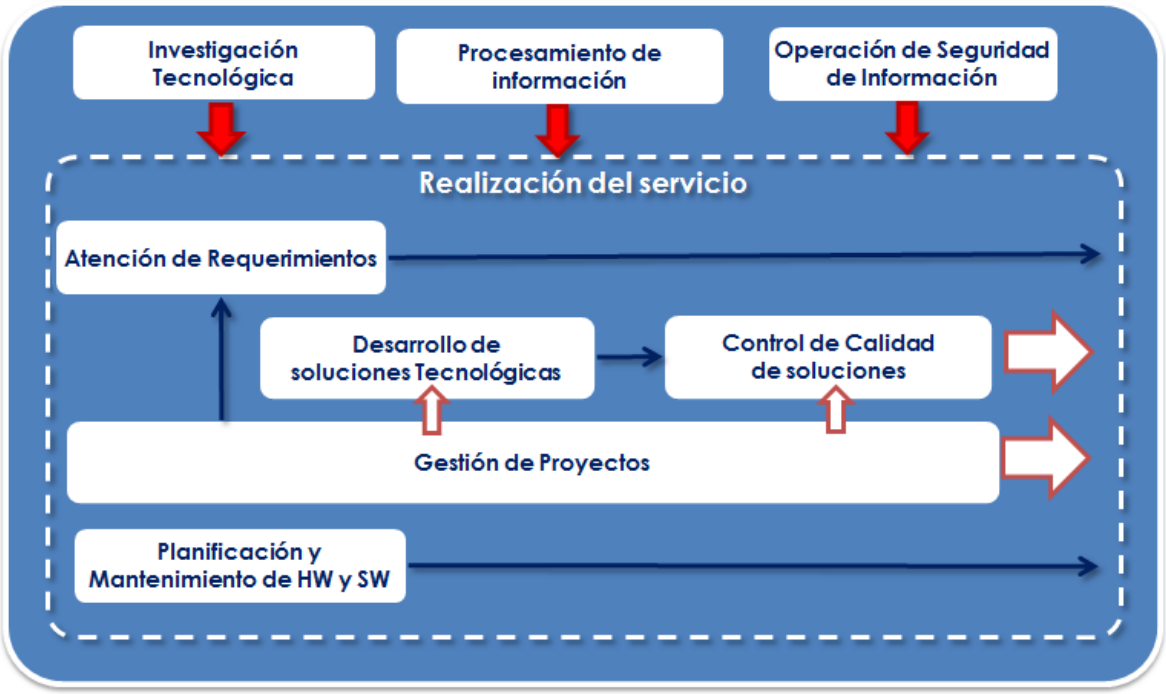
a) Desarrollo [47]



	Procesos	Subprocesos	
		Desarrollo	Doc. Soporte
Macroproceso Operativo	Planificación de soluciones	Gestión de Proyectos	Procedimiento
	Desarrollo de soluciones tecnológicas	Desarrollo de Software	Ficha
	Control de calidad de soluciones	Control de Calidad de Software	Procedimiento
	Planificación y mantenimiento de HW y SW		
	Atención de requerimientos	Atención de Requerimientos	Ficha
	Procesamiento de información		
	Operación de seguridad de información		
	Investigación tecnológica	Investigación de Tecnologías	Ficha

[47] Elaboración: los autores

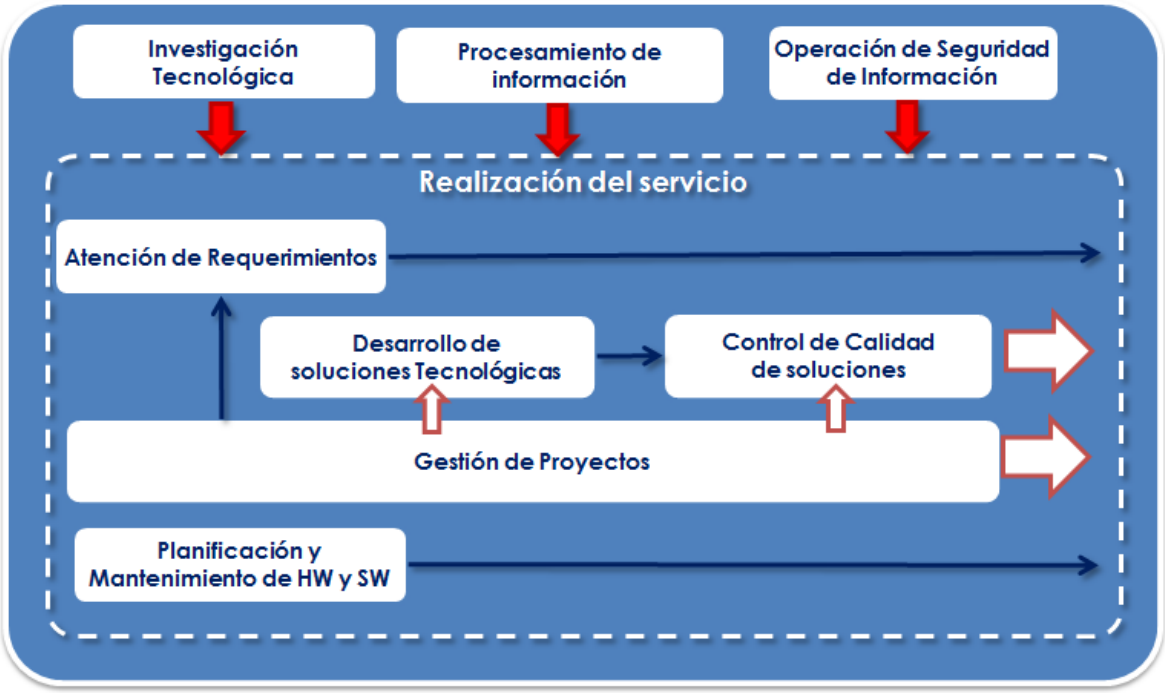
b) Business intelligence [48]



	Procesos	Subprocesos	
		Business Intelligence	Doc. Soporte
Macroproceso Operativo	Planificación de soluciones	Gestión de Proyectos	Procedimiento
	Desarrollo de soluciones tecnológicas	Desarrollo de Datamarts	Procedimiento
		Desarrollo de Dashboard	Procedimiento
		Desarrollo Proyectos Integrales	Procedimiento
	Control de calidad de soluciones	Control de Calidad BI	Ninguno
	Planificación y mantenimiento de HW y SW		
	Atención de requerimientos	Atención de Requerimientos	Procedimiento
	Procesamiento de información		
	Operación de seguridad de información		
	Investigación tecnológica	Investigación de Tecnologías	Ficha
		Análisis de Información	Ficha

[48] Elaboración: los autores

c) Centro de cómputo [49]

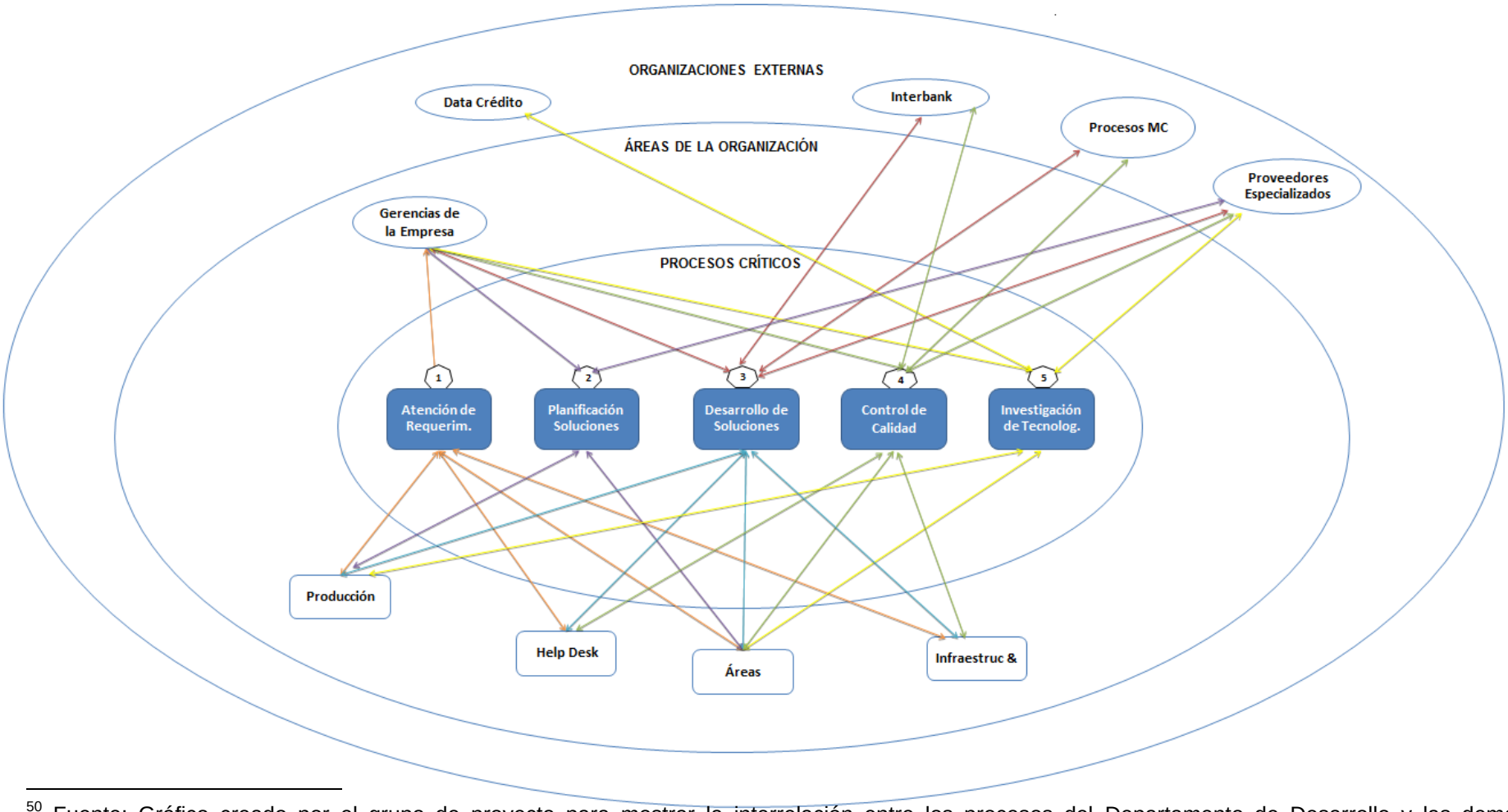


	Procesos	Subprocesos	
		Centro de Cómputo	Doc. Soporte
Macroproceso Operativo	Planificación de soluciones	Gestión de Proyectos	Ninguno
	Desarrollo de soluciones tecnológicas	Desarrollo de Tec. Hardware	Ficha
		Desarrollo de Tec. Software	
	Control de calidad de soluciones	Control de Calidad de Tecnologías	Ninguno
	Planificación y mantenimiento de HW y SW	Planificación de Mantenimiento de HW y SW	Ficha
	Atención de requerimientos	Atención de Requerimientos	Procedimiento
	Procesamiento de información	Procesamiento de Información	Ficha / Instructivos
	Operación de seguridad de información	Seguridad Perimetral	Ficha
		Back UP	Ficha
	Investigación tecnológica	Investigación de Tecnologías	Ficha

[49] Elaboración: los autores

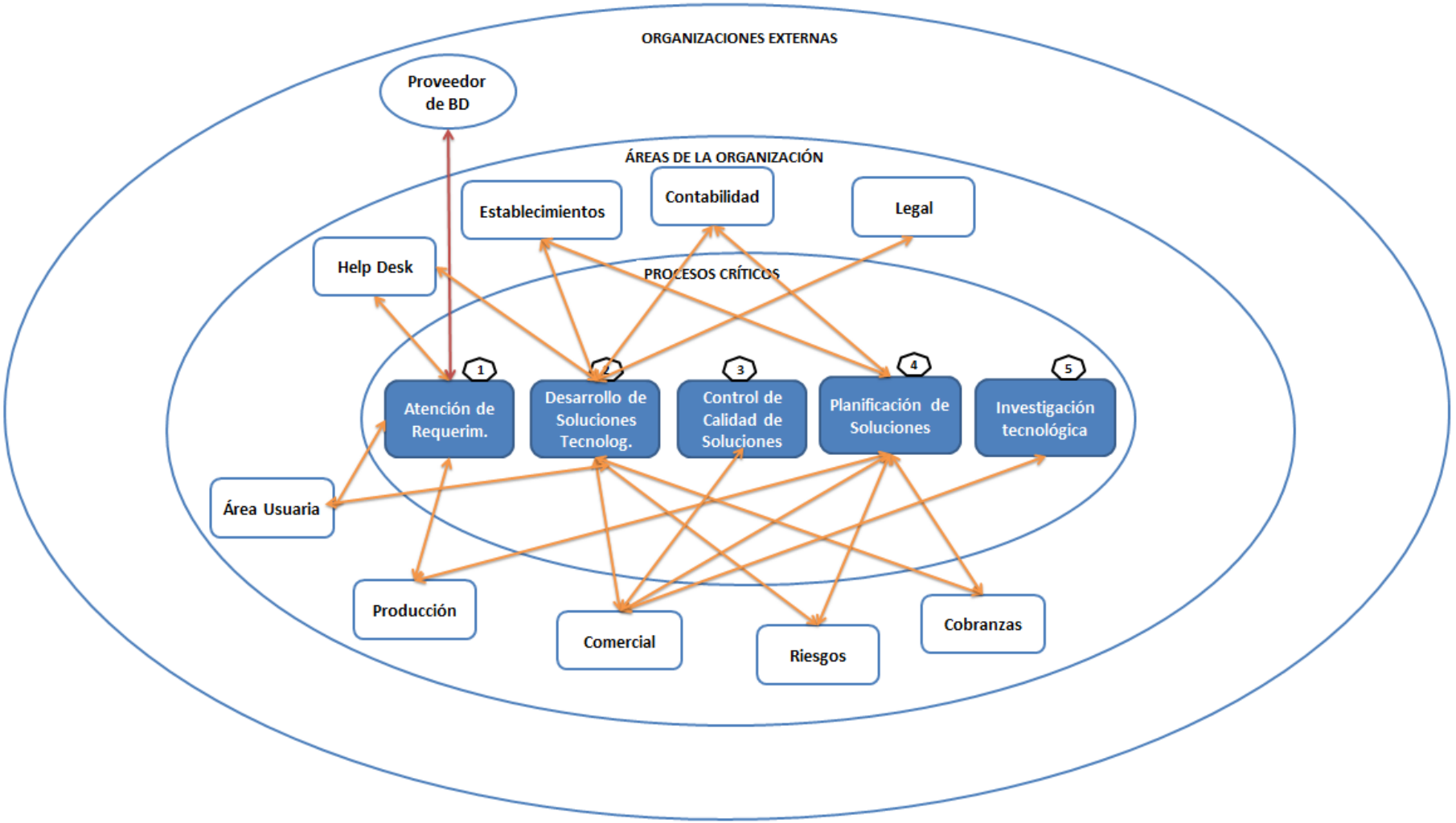
B) Identificación de activos

a) Desarrollo [50]



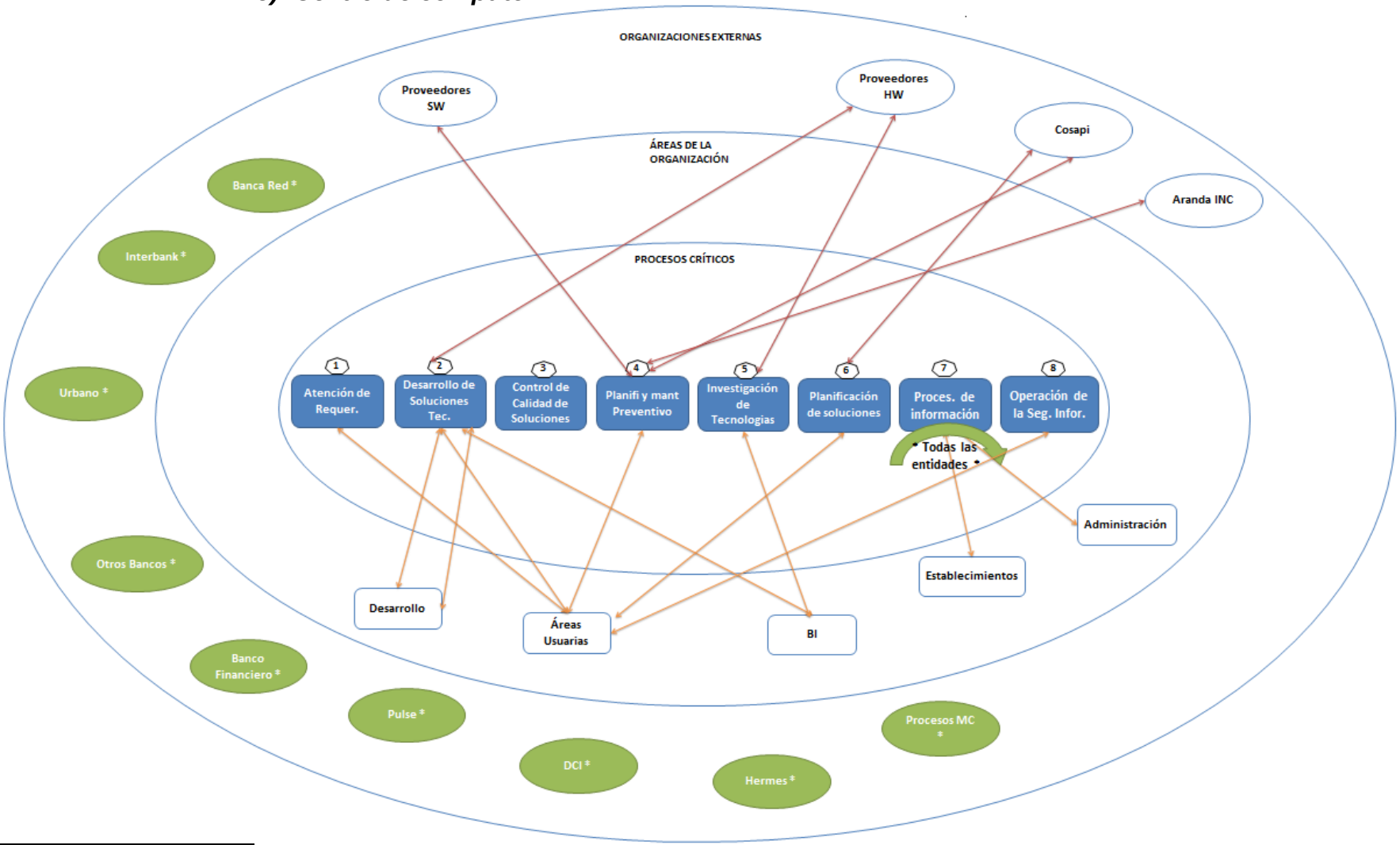
[50] Fuente: Gráfico creado por el grupo de proyecto para mostrar la interrelación entre los procesos del Departamento de Desarrollo y las demás dependencias de la empresa.

b) Business intelligence [51]



[51] Fuente: Gráfico creado por el grupo de proyecto para mostrar la interrelación entre los procesos del Departamento de Business Intelligence y las demás dependencias de la empresa.

c) *Centro de cómputo* [52]



[52] Fuente: Gráfico creado por el grupo de proyecto para mostrar la interrelación entre los procesos del Departamento de Centro de Cómputo y las demás dependencias de la empresa.

C) Inventario de activos

a) Inventario de activo: Desarrollo

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE INFORMACIÓN											
1	Cartillas	**I1**			**X**				**X**	Z:\Carpeta del Proyecto	Comité del proyecto y Terceros	Producción	JD			**X**	**X**		**X**	**X**	
2	Cotizaciones	**I1**		**X**					**X**	Z:\Carpeta del Proyecto	TI	Producción	JP			**X**	**X**	**X**	**X**		**X**
3	Procedimientos de negocio	**I1**			**X**				**X**	Site de Procesos	Usuarios empresa	Producción	Procesos			**X**					**X**
4	Documentación atención al cliente - Asignación	**I1**		**X**					**X**	Z:\Carpeta del Proyecto	Usuarios empresa	Producción	TI			**X**	**X**		**X**	**X**	
5	Documentación atención al cliente - desarrollo	**I1**		**X**					**X**	Z:\Carpeta del Proyecto	Usuarios empresa	Producción	TI			**X**	**X**		**X**	**X**	
6	Documentación atención al cliente - despliegue	**I1**		**X**					**X**	Z:\Carpeta del Proyecto	Usuarios empresa	Producción	TI			**X**	**X**		**X**	**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE INFORMACIÓN											
7	Documentación planificación de soluciones	I1		X					X	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			X		X			
8	Documentación Desarrollo de soluciones - análisis	I1		X	X				X	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			X		X	X		
9	Documentación desarrollo de soluciones - diseño	I1		X	X				X	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			X		X	X		
10	Documentación desarrollo de soluciones - desarrollo	I1		X					X	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			X		X	X		
11	Documentación desarrollo de soluciones - pruebas	I1		X					X	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			X		X	X		
12	Documentación desarrollo de soluciones - despliegue	I1		X					X	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			X		X	X		
13	Documentación control de calidad de soluciones - iniciación	I1		X					X	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			X			X	X	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE INFORMACIÓN											
14	Documentación control de calidad de soluciones - elaboración	**I1**		**X**					**X**	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			**X**		**X**	**X**	**X**	
15	Documentación control de calidad de soluciones - ejecución	**I1**		**X**					**X**	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			**X**		**X**	**X**	**X**	
16	Documentación control de calidad de soluciones - aceptación	**I1**		**X**					**X**	Z:\Carpeta del Proyecto	Comité del proyecto	Producción	JP			**X**			**X**	**X**	
17	Documentación investigación de tecnologías	**I1**		**X**	**X**				**X**	Z:\Carpeta del Proyecto	TI	Producción	JP, JD, GTI			**X**					**X**

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE SOFTWARE											
18	.Net, ASP	**SW1**							**X**	PC	Programador Analista	Networking	Producción			**X**	**X**		**X**	**X**	
19	Convertidor a PDF	**SW1**							**X**	PC	GTI	Help Desk	Help Desk			**X**	**X**	**X**	**X**	**X**	**X**
20	Correo	**SW1**				**X**				Servidor	Usuarios empresa	Networking	Producción		**X**		**X**	**X**	**X**	**X**	**X**
21	Drupal	**SW1**							**X**	Servidor	Programador Analista	Networking	Producción	**X**			**X**		**X**	**X**	
22	Eclipse (Java)	**SW1**				**X**				PC	JP Programador Analista	Help Desk	Producción			**X**	**X**		**X**	**X**	
23	Erwin	**SW1**				**X**				PC	JP Programador Analista	Help Desk	Producción			**X**			**X**		
24	Excel	**SW1**				**X**				PC	Usuarios empresa	Help Desk	Producción		**X**		**X**	**X**	**X**	**X**	**X**

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE SOFTWARE											
25	iSeries	**SW1**				**X**				Servidor	JP Programador Analista	Producción	Producción	**X**			**X**	**X**	**X**	**X**	
26	MySQL	**SW1**							**X**	Servidor	JP Programador Analista	Networking	Producción	**X**			**X**		**X**	**X**	
27	DB2	**SW1**							**X**	Servidor	JP Programador Analista	Networking	Producción	**X**			**X**		**X**	**X**	
28	Open Project	**SW1**				**X**				PC	JP Programador Analista	Help Desk	Producción			**X**		**X**			
29	PC Virtuales	**SW5**							**X**	PC	JP, Analista de Calidad	Help Desk	Producción			**X**	**X**		**X**	**X**	
30	MS Project	**SW1**				**X**				PC	JP JD	Help Desk	Producción			**X**		**X**	**X**	**X**	
31	Sistema de requerimientos	**SW3**				**X**				Servidor	JP JD	Help Desk	Producción			**X**	**X**	**X**			

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE SOFTWARE											
32	Visio	**SW1**				**X**				PC	JP Programador Analista	Help Desk	Producción			**X**	**X**		**X**	**X**	
33	Visual Basic	**SW1**				**X**				PC	JP Programador Analista	Help Desk	Producción			**X**	**X**		**X**	**X**	
34	Word	**SW1**				**X**				PC	Usuarios empresa	Help Desk	Producción	**X**			**X**	**X**	**X**	**X**	**X**
35	Cristal Report	**SW1**				**X**				PC	Usuarios empresa	Help Desk	Producción	**X**			**X**	**X**	**X**	**X**	**X**
36	MS Acces	**SW1**				**X**				PC	Usuarios empresa	Help Desk	Producción	**X**			**X**	**X**	**X**	**X**	**X**
37	RPG	**SW1**				**X**				PC	Usuarios empresa	Help Desk	Producción			**X**	**X**		**X**	**X**	
38	Desarrollos terciarizados	**SW1**				**X**				Servidor	Usuarios empresa	Producción	Producción	**X**			**X**	**X**	**X**	**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE SOFTWARE											
39	Aplicativos Visual Basic	**SW1**				**X**				Servidor	Usuarios empresa	Producción	Producción	**X**			**X**	**X**	**X**	**X**	
40	Aplicativos JAVA	**SW1**				**X**				Servidor	Usuarios empresa	Producción	Producción	**X**			**X**	**X**	**X**	**X**	
41	Aplicativos .NET	**SW1**				**X**				Servidor	Usuarios empresa	Producción	Producción	**X**			**X**	**X**	**X**	**X**	
42	MS Office	**SW1**				**X**				PC	Usuarios empresa	Help Desk	Producción			**X**	**X**		**X**	**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE HARDWARE											
43	PC	**F1**				**X**				Oficina	Usuarios empresa	Usuario	Help Desk		**X**		**X**	**X**	**X**	**X**	**X**
44	Serv. Java desarrollo	**F1**				**X**				Sala Servidores	Usuarios empresa	Producción	Producción			**X**	**X**		**X**	**X**	
45	Servidor AS400 desarrollo	**F1**				**X**				Sala Servidores	Usuarios empresa	Desarrollo	Producción			**X**	**X**		**X**	**X**	
46	Servidor AS400 producción	**F1**				**X**				Sala Servidores	Usuarios empresa	Producción	Producción	**X**			**X**		**X**		
47	Servidor de correo	**F1**				**X**				Sala Servidores	Usuarios empresa	Producción	Producción	**X**			**X**	**X**	**X**	**X**	**X**
48	Servidor Linux desarrollo	**F1**				**X**				Sala Servidores	Usuarios empresa	Desarrollo	Producción			**X**	**X**		**X**	**X**	
49	Servidor Linux producción	**F1**				**X**				Sala Servidores	Usuarios empresa	Producción	Producción	**X**			**X**		**X**		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE HARDWARE											
50	Servidor Web desarrollo	**F1**				**X**				Sala Servidores	Usuarios empresa	Desarrollo	Producción			**X**	**X**	**X**	**X**	**X**	
51	Servidor Web producción	**F1**				**X**				Sala Servidores	Usuarios empresa	Producción	Producción	**X**			**X**		**X**		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										SERVICIOS (TERCEROS)											
52	Internet	**S1**								Sala Servidores	Usuarios empresa	Networking	Producción	**X**			**X**	**X**	**X**	**X**	**X**
53	Telefonía claro	**S1**								Oficina	Usuarios empresa	Networking	Producción	**X**			**X**	**X**	**X**	**X**	**X**
54	Celular claro	**S1**								Oficina	Usuarios empresa	Networking	Producción			**X**	**X**	**X**	**X**	**X**	**X**
55	Servicio procesos MC	**S1**				**X**				Oficina	Usuarios empresa	Networking	Producción	**X**			**X**	**X**	**X**		
56	Servicio Global Net	**S1**				**X**				Oficina	Usuarios empresa	Networking	Producción	**X**			**X**	**X**	**X**		
57	Servicio Data Crédito	**S1**					**X**			Oficina	Usuarios empresa	Networking	Producción	**X**			**X**	**X**	**X**		
58	Servicio cobranza: Tec Center y Pague Ya	**S1**				**X**				Oficina	Usuarios empresa	Networking	Producción		**X**		**X**	**X**	**X**		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										SERVICIOS (TERCEROS)											
59	Servicio Certicon	**S1**					**X**		**X**	Oficina	Usuarios empresa	Networking	Producción			**X**	**X**	**X**	**X**		
60	Servicio Infocor	**S1**					**X**		**X**	Oficina	Usuarios empresa	Networking	Producción			**X**	**X**	**X**	**X**		
61	DCI: Global Vision	**S1**				**X**				Oficina	Usuarios empresa	Networking	Producción	**X**			**X**	**X**	**X**		
62	DCI: Consumos Internacionales - facturación	**S1**				**X**				Oficina	Usuarios empresa	Networking	Producción		**X**		**X**	**X**	**X**		
63	Discover: Pulse	**S1**				**X**				Oficina	Usuarios empresa	Networking	Producción		**X**		**X**	**X**	**X**		
64	Servicio IATA	**S1**				**X**				Oficina	Usuarios empresa	Networking	Producción		**X**		**X**	**X**	**X**		
65	Procesos de Recaudación: Financiero, Scotian, Continental, Crédito, Comercio, Interbank y BIF	**S1**				**X**				Oficina	Usuarios empresa	Networking	Producción	**X**			**X**	**X**	**X**		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										SERVICIOS (TERCEROS)											
66	Proceso de Cargo en cuenta: Crédito, Scotiabank y Continental	**S1**					**X**		**X**	Oficina	Usuarios empresa	Networking	Producción		**X**		**X**	**X**	**X**		
67	Central Crediticia RCC	**S1**						**X**		Oficina	Usuarios empresa	Networking	Producción		**X**		**X**	**X**	**X**		
68	Servicio de Urbano	**S1**					**X**			Oficina	Usuarios empresa	Networking	Producción		**X**		**X**	**X**	**X**		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										COLABORADORES											
69	Analista de Calidad (QA)													X			X		X	X	
70	Analista Programador Junior (APJ)													X			X		X		
71	Analista Programador Senior (APS)													X			X		X		X
72	Arquitecto (ARQ)													X				X	X		X
73	Jefe de Desarrollo (JD)													X			X	X		X	X
74	Jefe de Proyecto (JP)													X			X	X	X	X	X
75	Practicante de Desarrollo (PD)																				

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										COLABORADORES											
76	Analista de Calidad (QA)													X			X		X	X	
77	Líder Usuario (LU)													X			X	X	X	X	
78	Operadores (OPE)													X			X		X		
79	Programador Junior (PROG)													X			X		X		
80	Programador Senior (PROGS)													X			X		X		
81	Soporte Técnico (ST)													X			X	X	X	X	
82	Networking (NT)													X					X		X

b) Inventario de activo: Business intelligence

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE INFORMACIÓN											
1	Documentación (Actas, avances)	**I1**		**X**			**X**			Sharepoint BI	BI	Coordinador BI	Coordinador BI			**X**		**X**	**X**	**X**	**X**
2	Documento de Análisis	**I1**		**X**			**X**			Sharepoint BI	BI	Coordinador BI	Coordinador BI	**X**			**X**	**X**		**X**	
3	Documento de Diseño	**I1**		**X**			**X**			Sharepoint BI	BI	Coordinador BI	Coordinador BI	**X**					**X**		
4	Documento de Despliegue	**I1**		**X**			**X**			Sharepoint BI	BI	Coordinador BI	Coordinador BI	**X**			**X**	**X**		**X**	
5	Documentación de Proyecto	**I1**		**X**			**X**			Sharepoint BI	BI	Coordinador BI	Coordinador BI						**X**		
6	Documentos de Análisis e Investigación	**I1**		**X**			**X**			Sharepoint BI	BI	Coordinador BI	Coordinador BI	**X**	**X**	**X**			**X**		**X**

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE INFORMACIÓN											
7	Bases de Datos Externas	I1	X				X				BI	Coordinador BI	Gerencias	X			X	X	X	X	
8	Datawarehouse_DC	I1	X			X				Servidor SQL BI	BI	Producción	Coordinador BI	X			X	X	X	X	
9	Datawarehouse_DT	I1	X			X				Servidor SQL BI	BI	Producción	Coordinador BI	X			X	X	X	X	
10	BDExt	I1	X				X			Servidor SQL BI	BI	Producción	Coordinador BI	X			X	X	X	X	
11	BDProspectos	I1	X			X				Servidor SQL BI	BI	Producción	Coordinador BI	X			X	X	X	X	
12	BDRCC	I1	X			X				Servidor SQL BI	BI	Producción	Coordinador BI	X			X	X	X	X	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE INFORMACIÓN											
13	Procedimientos de Negocio	**I1**		**X**			**X**			Sharepoint	BI	Coordinador BI					**X**	**X**		**X**	
14	Indicadores	**I1**		**X**		**X**					BI	Coordinador BI	Coordinador BI	**X**			**X**	**X**		**X**	
15	Dashboard	**I1**		**X**		**X**					BI	Coordinador BI	Coordinador BI	**X**				**X**		**X**	
16	BSC	**I1**		**X**			**X**				BI	Coordinador BI	Coordinador BI	**X**			**X**	**X**	**X**	**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE SOFTWARE											
17	Access	**SW1**					**X**			PC	BI	BI	Centro Cómputo	**X**			**X**	**X**	**X**	**X**	
18	Erwin	**SW1**					**X**			Infoteca	BI	BI	Centro Cómputo	**X**			**X**	**X**		**X**	
19	Excel	**SW1**				**X**				PC	BI	BI	Centro Cómputo	**X**			**X**	**X**	**X**	**X**	**X**
20	Live Office	**SW1**				**X**				PC	BI	BI	Centro Cómputo	**X**				**X**		**X**	
21	MS Office	**SW1**				**X**				PC	BI	BI	Centro Cómputo	**X**			**X**	**X**	**X**	**X**	**X**
22	Xcelsius 2008	**SW1**					**X**			PC	BI	BI	Centro Cómputo	**X**			**X**	**X**		**X**	
23	Consola de Administración Central del BO	**SW1**					**X**			PC	BI	BI	Centro Cómputo	**X**				**X**		**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE SOFTWARE											
24	Outlook	**SW1**				**X**				PC	BI	BI	Centro Cómputo		**X**		**X**	**X**	**X**	**X**	**X**
25	Licencia SAP BO	**SW1**				**X**				PC	BI	BI	BI	**X**			**X**	**X**	**X**	**X**	
26	Infoview	**SW1**				**X**				PC	BI	Centro Cómputo	Centro Cómputo	**X**			**X**	**X**		**X**	
27	ETL AS400	**SW3**				**X**				PC	BI	BI	Centro Cómputo	**X**				**X**		**X**	
28	ETL SQL	**SW3**				**X**				PC	BI	BI	BI	**X**				**X**		**X**	
29	Programas de Base de Datos	**SW1**				**X**				PC	BI	BI	BI	**X**			**X**	**X**		**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE SOFTWARE											
30	Jobs AS400	**SW3**				**X**				PC	BI	BI	BI	**X**			**X**	**X**		**X**	
31	SAP Business Objects	**SW1**				**X**				PC	BI	BI	Centro Cómputo	**X**			**X**	**X**	**X**	**X**	
32	Sistema AS/400	**SW1**					**X**				BI	Centro Cómputo	Centro Cómputo	**X**			**X**	**X**		**X**	
33	Sistema de Control de Cambios AS/400	**SW3**					**X**				BI	BI	Centro Cómputo			**X**	**X**	**X**		**X**	
34	SQL Server 2008	**SW1**				**X**					BI	Producción	Centro Cómputo	**X**			**X**	**X**	**X**	**X**	
35	VS Integration Services	**SW1**				**X**					BI	BI	Centro Cómputo	**X**			**X**	**X**	**X**	**X**	
36	Macros	**SW1**				**X**					BI	BI	Centro Cómputo	**X**			**X**	**X**	**X**	**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE HARDWARE											
37	Anexo	**F5**				**X**				Escritorio	BI	BI	Centro de Computo		**X**		**X**	**X**	**X**	**X**	
38	Computadoras	**F1**				**X**				Escritorio	BI	BI	Centro de Computo	**X**			**X**	**X**	**X**	**X**	
39	Servidor de Desarrollo	**F1**				**X**				Producción	BI	Producción	Centro de Computo	**X**			**X**	**X**		**X**	
40	Servidor de Producción	**F1**				**X**				Producción	BI	Producción	Centro de Computo	**X**			**X**	**X**		**X**	
41	SVRSQLBI	**F1**				**X**				Producción	BI	Producción	Centro de Computo	**X**			**X**	**X**	**X**	**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										ACTIVOS DE HARDWARE											
42	SVRBIPRO	**F1**				**X**				Producción	BI	Producción	Centro de Computo	**X**			**X**	**X**	**X**	**X**	
43	SVRRCC	**F1**				**X**				Producción	BI	Producción	Centro de Computo	**X**			**X**	**X**	**X**	**X**	

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	VALOR			PROCESO RELACIONADO				
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					Alto	Medio	Bajo	1	2	3	4	5
										COLABORADORES											
44	Analista BI														X		X	X	X	X	X
45	Coordinador BI													X			X	X	X	X	X
46	Desarrollador BI														X		X	X	X	X	
47	Líder de Proyecto													X				X	X		
48	Líder Usuario													X				X	X		
49	Patrocinador de Proyecto														X			X	X		

c) Inventario de activo: Centro de cómputo

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE INFORMACIÓN										
1	Bitácora de procesos diarios	I2	X			X				Producción	Operador	Jefe de Producción	Jefe de Producción							X
2	Reportes especies valoradas(fact, N/C, bolet, cheques, claves)	I2	X				X			Producción	Usuarios Emisión y Distribución	Jefe de Producción	Jefe de Operaciones							X
3	Reportes cierre diario	I2	X			X				Producción	Operador	Jefe de Producción	Jefe de Producción							X
4	Informe del Proyecto	I2		X					X	Servidor de Archivos	Usuarios Centro de Computo	Coordinador I & N	Jefe Centro de Computo		X					
5	Documentación del proyecto	I2		X					X	Servidor de Archivos	Usuarios Centro de Computo	Coordinador I & N	Jefe Centro de Computo		X					
6	Orden de compra	I2		X					X	I & N	Usuarios Centro de Computo	Coordinador I & N	Jefe Centro de Computo		X					

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE INFORMACIÓN										
7	Acta de Reunión	I1		X					X	Servidor de Archivos	Usuarios Centro de Computo	Coordinador I & N	Jefe Centro de Computo		X		X			
8	Informe de propuesta	I1	X						X	Servidor de Archivos	Usuarios Centro de Computo	Coordinador I & N	Jefe Centro de Computo				X			
9	Contratos de Mantenimiento	I2		X			X			Asistentes de Gerencia	Usuarios Centro de Computo	Coordinador I & N	Gerencia TI		X					
10	Contratos de Soporte	I2		X			X			Servidor de Archivos	Usuarios Centro de Computo	Coordinador I & N	Jefe Centro de Computo		X					
11	Documentación de prueba	I1		X					X	Servidor de Archivos	Usuarios Centro de Computo	Coordinador I & N	Jefe Centro de Computo				X			
12	Documentación de tecnología	I1	X						X	Servidor de Archivos	Usuarios Centro de Computo	Coordinador I & N	Jefe Centro de Computo	X	X	X	X	X		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7
										ACTIVOS DE INFORMACIÓN										
13	Inventario de HW y SW	I1		X			X			I & N	Coordinador I & N	Coordinador I & N	Coordinador I & N					X		
14	Licencia de Tecnología	I1	X					X		I & N	Coordinador I & N	Coordinador I & N	Coordinador I & N	X	X	X	X	X		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7
										ACTIVOS DE SOFTWARE										
16	BD DB2	SW0				X				Servidor AS400 Producción/Desarrollo	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
17	Aranda Service Desk	SW1				X				BladeCenter/SvrAranda	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X		X	X		
18	MS Office	SW1				X				Computador	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
19	Exchange	SW1				X				BladeCenter/SvrMail	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
20	Antivirus Kaspersky	SW1				X				BladeCenter/SvrKaspersky	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X		
21	Netsupport	SW1				X				Computador	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X					X	
22	VMWARE Wesphere	SW1				X				BladeCenter/SvrCenter	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE SOFTWARE										
23	BD Oracle	SW0				X				Servidor HP Bridge	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
24	BD My SQL	SW0				X				BladeCenter/SvrMySql	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
25	BD Sybase	SW0				X				BladeCenter/SvrSybase	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
26	S.O. Windows Server Estándar	SW0				X				Servidores	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
27	S.O. Linux Redhat	SW0				X				SvrLinux	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
28	S.O. Unix	SW0				X				Servidor HP Bridge	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
29	S.O. OS/2	SW0				X				Servidor AS400 Producción/Desarrollo	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE SOFTWARE										
30	Filtro Web Barracuda	SW1				X				Producción	Usuarios I & N	TI	Jefe Centro de Computo	X						X
31	Antispam Symantec	SW1				X				Producción	Usuarios I & N	TI	Jefe Centro de Computo	X					X	
32	Page Device Control	SW1				X				Producción	Usuarios I & N	TI	Jefe Centro de Computo	X						
33	Vision	SW2				X				Servidor AS400 Producción/Desarrollo	Operador Producción	TI	Jefe Centro de Computo						X	X
34	Business Object	SW2				X				BladeCenter/SvrBIPRO	Usuarios Centro de Computo	TI	Coordinador BI	X						X
35	Drupal	SW2				X				SvrLinux	Usuarios I & N	TI	Gerencia Comercial	X						X
36	Aranda Inventory	SW1					X			BladeCenter/SvrAranda	Usuarios I & N	TI	Jefe Centro de Computo					X		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE SOFTWARE										
37	Subversion	SW1				X				BladeCenter/SvrSubversion	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
38	MOC	SW3				X				BladeCenter/SvrFile	Operador Producción	TI	Jefe de Establecimientos							X
39	MAG	SW3				X				BladeCenter/SvrFile	Operador Producción	TI	Jefe de Establecimientos							X
40	MCR	SW3				X				BladeCenter/SvrFile	Operador Producción	TI	Jefe de Establecimientos							X
41	CADWEB	SW3				X				BladeCenter/Svr	Operador Producción	TI	Jefe de Establecimientos							X
42	CPCobranzas (recaudadoras y cartas)	SW3				X				BladeCenter/SvrFile	Operador Producción	TI	Jefe de Cobranzas							X
43	Estado cuenta web (generación de pdf's)	SW3				X				BladeCenter/SvrFile	Operador Producción	TI	Jefe Centro de Computo							X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS SOFTWARE										
44	Bridge (aplicativo recepción y envío de lote a DCI)	SW2				X				Servidor HP Bridge	Operador Producción	TI	Jefe Centro de Computo							X
45	SIAF	SW3				X				BladeCenter/SvrFile	Operador Producción	TI	Jefe de Canales							X
46	Emisión de EECC y Doc. Aut. (Generación txt para Urbano)	SW3				X				BladeCenter/SvrFile	Operador Producción	TI	Jefe de Canales							X
47	Control de Acceso	SW2				X				BladeCenter/SvrFile	Usuarios Centro de Computo	TI	Jefe Centro de Computo						X	X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE HARDWARE										
48	Servidor AS400 Producción	F1				X				Producción	Operador Producción	TI	Jefe Centro de Computo	X						X
49	Servidor AS400 Desarrollo	F1				X				Producción	Operador Producción	TI	Jefe Centro de Computo	X						X
50	Impresora	F5				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
51	Teléfono	F2				X				Producción/ I & N / Help Desk	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
52	Firewall JUNIPER	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X					X	X
53	Laptop	F1				X				I & N / Help Desk	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						
54	Periféricos	F3							X	I & N / Help Desk	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE HARDWARE										
55	Servidor de Correo Exchange	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
56	Servidor de Directorio Activo	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
57	Servidor de Archivos	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
58	Servidor Web Desarrollo	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						
59	Servidor Web Producción	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X			X			
60	Servidor Linux Desarrollo	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
61	Servidor Linux Producción	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE HARDWARE										
62	Servidor Sybase	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
63	Servidor Avaya	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
64	Servidor BI	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
65	Servidor BI SQL	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
66	Servidor Card al Día	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
67	Servidor EPM	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						
68	Servidor HP Bridge	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE HARDWARE										
69	Routers	F2				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
70	Switch	F2				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
71	Patch Panel	F2				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
72	Central telefónica Nortel	F2				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
73	Central telefónica Avaya	F2				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
74	Black Berry	F2				X				Usuarios BlackBerry	Usuarios Centro de Computo	TI	Jefe de Administración	X	X	X	X	X	X	X
75	HSM Thales Producción	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE HARDWARE										
76	HSM Thales Desarrollo	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
77	HSM Atalla Producción	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
78	HSM Atalla Desarrollo	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
79	DSC 300 Storage	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
80	Servidor Intranet	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
81	Servidor BI Desarrollo	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
82	Cámaras Vigilancia	F5				X				Producción	Usuarios Centro de Computo	TI	?	X						X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE HARDWARE										
83	Servidor CCTV	F5				X				Producción	Usuarios Centro de Computo	TI	?	X						X
84	Servidor Back UP	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
85	Unidades de cinta LTO4	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
86	Unidades de cinta LTO3	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
87	Servidor de Impresoras	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
88	UPS	F5				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
89	Disco duro externo	F3							X	I & N	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										ACTIVOS DE HARDWARE										
90	RACK	F4				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
91	Triturador de papel	F5							X	Producción	Usuarios Centro de Computo	TI	Jefe de Administración							X
92	DLO Back UP					X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						X
93	Modem Claro	F2							X	Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X						
94	Computadoras	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo	X	X	X	X	X	X	X
95	Control de Acceso	F5				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo						X	X
96	Unidad de cinta SQRL	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo							X

97	Unidad de cinta HP	F1				X				Producción	Usuarios Centro de Computo	TI	Jefe Centro de Computo						X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										SERVICIOS (TERCEROS)										
98	Internet CLARO	S1				X				Producción	?	TI	CLARO	X	X	X	X	X		
99	Trafic view	S1				X				Página web CLARO	?	TI	CLARO	X						X
100	Telebanking (Scotiacargos)	S1				X				Página web SCOTIABANK	?	TI	SCOTIABANK							X
101	Teletransfer (BCP)	S1				X				Página web BCP	?	TI	BCP							X
102	Servidor FTP Banco Financiero	S1				X				Producción	?	FINANCIERO	FINANCIERO							X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										SERVICIOS (TERCEROS)										
103	Hermes custodia de medios magnéticos	S2				X	X			HERMES	?	TI	HERMES							X
104	Tarjeta Token (BCP)	S1				X				Producción	?	TI	Producción							X
105	Servidor FTP Urbano	S1				X				Producción	?	URBANO	URBANO							X
106	Servidor FTP Procesos MC	S1				X				Producción	?	PROCESOS MC	PROCESOS MC							X
107	BANCARED	S1				X				Producción	?	BANCARED	BANCARED							X
108	PROCESOS MC	S1				X				Producción	?	PROCESOS MC	PROCESOS MC							X
109	GLOBALNET INTERBANK	S1				X				Producción	?	INTERBANK	INTERBANK							X

110	DCISC	S1				X				Producción	?	DCISC	DCISC						X

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										COLABORADORES										
111	Coordinador de I&N													X	X		X	X	X	
112	Administrador de Red													X	X		X	X	X	
113	Usuarios													X	X	X	X		X	X
114	Jefe de Producción													X					X	X
115	Analista de Help Desk													X	X	X	X	X		

ÍTEM	NOMBRE DEL ACTIVO	CATEGORÍA	CLASIFICACIÓN			FRECUENCIA USO				UBICACIÓN FÍSICA/LÓGICA	USUARIO	CUSTODIO	PROPIETARIO (RESPONSABLE)	PROCESO RELACIONADO						
			CONFIDENCIAL	USO INTERNO	PUBLICO	DIARIO	MENSUAL	ANUAL	OTRO					1	2	3	4	5	6	7,8
										COLABORADORES										
116	Jefe Centro de Cómputo													X	X	X	X	X	X	X
117	Jefe de Desarrollo													X						X
118	Operador de Producción													X						X
119	Asistente Help Desk													X	X	X	X	X		

D) Análisis y evaluación de riesgos

a) Análisis y evaluación de riesgos: Desarrollo

			¿Qué afecta?						Riesgo Efectivo			
Nro.	**ACTIVOS AFECTADOS**	**AMENAZA**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valoración**	**VULNERABILIDADES**	**Mecanismos de protección existentes**	**Probabilidad**	**Impacto**	**Riesgo**	**Tolerancia**
RIESGOS DE LOS ACTIVOS DE INFORMACIÓN												
1	Cotizaciones	Fuga/Divulgación de información por parte del personal interno	**1**	**1**	**2**	**4**	-No existe política de Seguridad de información documentada -Se desconoce si se tiene formalizada la solicitud de acuerdos de confidencialidad con proveedores -No se tienen definidos las ubicaciones de las cotizaciones.	-Centralizar la información electrónica -Efectuar el respaldo de la información -Control de acceso a la información -Restaurar información	1	2	**6**	**TT**
		Modificación de información - accidental / Intencional							1	2	**6**	**TT**
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)							1	2	**6**	**TT**
		Pérdida parcial o completa de información							2	2	**8**	**TT**
2	- Procedimientos de Negocio - Cartilla	Fuga/Divulgación de información por parte del personal interno	**1**	**3**	**3**	**7**	-No se cuenta con cultura de revisión, actualización y seguridad de los procesos y procedimientos por los usuarios. -No se cuenta con cultura de revisión de los procesos y procedimientos por el personal del Dpto.	-Centralizar la información electrónica -Definir niveles de acceso asociado a perfiles de usuarios -Efectuar el respaldo de la información -Control de acceso a la información	1	2	**9**	**TT**
		Modificación de información - accidental / Intencional							2	1	**9**	**TT**
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)							1	2	**9**	**TT**

		Pérdida parcial o completa de información						-Restaurar información	1	1	**8**	TT
3	Documentación Atención al cliente -Asignación -Desarrollo -Despliegue	Fuga/Divulgación de información por parte del personal interno	**3**	**3**	**3**	**9**	- No existe políticas, cartas u otros documentos que evidencien confidencialidad de información.	-Efectuar el respaldo de la información -Respaldar las cintas de backup en lugar adecuado -Control de acceso a la información -Restaurar información	2	4	**17**	RT
		Ejecución errónea del proceso de RQ por el usuario y personal de Desarrollo					- No se cuenta con metodología o procedimiento formal -Desconocimiento de la metodología por los usuarios de la empresa		2	4	**17**	RT
		Accesos no autorizados					- No se cuenta con el control de accesos configurado por usuario.		2	4	**17**	RT
		Robo de documentación					- Los documentos son fácilmente extraíbles		2	4	**17**	RT
		Información desactualizada / No disponible					-No contar un procedimiento para actualización de información		2	4	**17**	RT
		Modificación de información - Accidental / Intencional Pérdida parcial / Completa de información					- No se cuenta con un Control adecuado sobre el acceso de los documentos - No se cuenta con Sistema de control de cambios/versiones		3	4	**21**	RT
4	Documentación Planificación de Soluciones	Fuga/Divulgación de información por parte del personal interno	**1**	**3**	**3**	**7**	- La metodología de Gestión de Proyectos no se encuentra aprobada. - No se cuenta con Sistema de control de versiones -Desconocimiento de la metodología por los usuarios de la empresa.	-Efectuar el respaldo de la información -Respaldar las cintas de backup en lugar adecuado -Control de acceso a la información -Restaurar información	1	2	**9**	TT
		Modificación de información - accidental / Intencional							2	1	**9**	TT
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)							1	2	**9**	TT
		Pérdida parcial o completa de información							1	2	**9**	TT

5	Documentación Desarrollo de Soluciones: - Análisis - Diseño - Desarrollo - Pruebas - Despliegue	Fuga/Divulgación de información por parte del personal interno	**3**	**3**	**3**	**9**	- No existe políticas, cartas u otros documentos que evidencien confidencialidad de información.	-Efectuar el respaldo de la información -Respaldar las cintas de backup en lugar adecuado -Control de acceso a la información -Restaurar información	3	4	**21**	**RT**
		Ejecución errónea del proceso por el usuario y personal de Desarrollo					- No se cuenta con metodología o procedimiento formal -Desconocimiento de la metodología por los usuarios de la empresa		2	5	**19**	**RT**
		Accesos no autorizados					- No se cuenta con el control de accesos configurado por usuario.		4	5	**29**	**NT**
		Robo de documentación					- Los documentos son fácilmente extraíbles		4	5	**29**	**NT**
		Error al realizar las pruebas unitarias					- Desconocimiento de métodos para ejecución de pruebas unitarias por parte de los desarrolladores.		2	4	**17**	**RT**
		Información desactualizada / No disponible					-No contar un procedimiento para actualización de información		2	4	**17**	**RT**
		Modificación de información - Accidental / Intencional Pérdida parcial / Completa de información					- No se cuenta con un Control adecuado sobre el acceso de los documentos - No se cuenta con Sistema de control de cambios/versiones		3	5	**24**	**RT**
6	Documentación Control de Calidad de soluciones - Iniciación - Elaboración - Ejecución - Aceptación	Fuga/Divulgación de información por parte del personal interno	**3**	**3**	**3**	**9**	- No existe políticas, cartas u otros documentos que evidencien confidencialidad de información.	-Efectuar el respaldo de la información -Respaldar las cintas de backup en lugar adecuado -Control de acceso a la información -Restaurar información	3	4	**21**	**RT**
		Ejecución errónea del proceso por el usuario					- Falta de compromiso de los usuarios en cumplimiento de la metodología de control de calidad.		2	4	**17**	**RT**
		Información desactualizada / No disponible					-No contar un procedimiento para actualización de		2	4	**17**	**RT**

							información						
		Accesos no autorizados					- No se cuenta con el control de accesos configurado por usuario.		3	5	**24**	RT
		Robo de documentación					- Los documentos son fácilmente extraíbles		3	5	**24**	RT
		Modificación de información - Accidental / Intencional Pérdida parcial / Completa de información					- No se cuenta con un Control adecuado sobre el acceso de los documentos - No se cuenta con Sistema de control de cambios/versiones		3	5	**24**	RT
7	Documentación Investigación de Tecnologías	Fuga/Divulgación de información por parte del personal interno	**1**	**2**	**3**	**6**	-No existe política de acuerdos de confidencialidad para el personal interno. -No se cuenta con ambiente independiente para pruebas de investigación.	-Control de acceso a la información -Restaurar información	1	2	**8**	TT
		Modificación de información - accidental							2	2	**10**	TT
		Modificación de información - intencional							2	1	**8**	TT
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)							2	1	**8**	TT
		Pérdida parcial o completa de información							2	2	**10**	TT

Cuadro 3.19: Análisis y evaluación de riesgos de departamento de desarrollo [53]

[53] Elaboración: los autores.

			¿Qué afecta?						Riesgo Efectivo			
Nro.	ACTIVOS AFECTADOS	AMENAZA	Confidencialidad	Integridad	Disponibilidad	Valoración	VULNERABILIDADES	Mecanismos de protección existentes	Probabilidad	Impacto	Riesgo	Tolerancia
RIESGOS DE LOS ACTIVOS DE SOFTWARE												
8	Herramientas y entornos de desarrollo: -.Net -Drupal -Eclipse (Java) -iSeries -Visual Basic -RPG	Mala instalación, configuración, actualización de software	**1**	**3**	**4**	**8**	- No existe con manuales de soporte para la solución de problemas (configuraciones, instalaciones y actualizaciones.)	-Todos los usuarios deben de contar con la misma versión de software -Registro de Aranda por errores que se presentan	2	3	**14**	TT
		Herramientas desactualizadas / no vigentes					-No se cuenta con el soporte para actualizar herramientas		2	3	**14**	TT
		Cambio de versión de las herramientas y entornos					-No se cuenta con un soporte para revisar el cambio de versión		2	4	**16**	RT
		Instalación de software no licenciados					-No se cuenta con un control para instalación de software no licenciado		2	5	**18**	RT
		Falta de renovación de licencias.					- El amarre de los desarrollos a las versiones del software.		2	5	**18**	RT
		Falta de licencias para el software					- Número limitado de licencias para los software		2	3	**14**	TT
		Eliminación de archivos propios del lenguaje					- Desconocimiento del personal de soporte para la solución de problemas (configuraciones y actualizaciones.)		2	3	**14**	TT
9	Correo	Mala instalación del software	**1**	**1**	**4**	**6**	-No existe uniformidad en las	-Todos los usuarios deben de	2	2	**10**	TT

		Infección por código malicioso, virus, troyanos, gusanos					versiones del cliente correo. -Impacto en los sistemas por actualización de versión del servidor de correo.	contar con la misma versión de software -Registro de Aranda por errores que se presentan	1	3	**3**	TT
		Falta de soporte técnico apropiado para el software							1	3	**9**	TT
		Modificación de la configuración por efecto utilizado por el software							1	3	**9**	TT
		Perdida de información por caída de correos							1	3	**9**	TT
		Eliminación de archivos de instalación del software							1	3	**9**	TT
		Acceso al software por usuarios no autorizados							1	3	**9**	TT
10	MS Office	Mala instalación del software	**1**	**1**	**4**	**6**	-No existe uniformidad en las versiones. -Impacto en los sistemas por actualización de versión	-Todos los usuarios deben de contar con la misma versión de software -Registro de Aranda por errores que se presentan	2	2	**10**	TT
		Infección por código malicioso, virus, troyanos, gusanos							2	2	**10**	TT
		Falta de soporte técnico apropiado para el software							2	2	**10**	TT
		Modificación de la configuración por efecto utilizado por el software							2	2	**10**	TT
		Corrupción de archivos							2	2	**10**	TT
		Eliminación de archivos de instalación del software							2	2	**10**	TT
		Acceso al software por usuarios no autorizados							2	2	**10**	TT
11	-Herramientas Case Erwin	Mala instalación del software	**1**	**2**	**3**	**6**	-Número limitado de licencias para los software -Impacto en los sistemas por actualización de versión	-Registro de Aranda por errores que se presentan	2	1	**8**	TT
		Infección por código malicioso, virus, troyanos, gusanos							2	2	**10**	TT
		Falta de soporte técnico apropiado para el software									**6**	TT
		Modificación de la configuración por efecto utilizado por el software							3	1	**9**	TT
		Falta de licencia para el software							3	1	**9**	TT
		Eliminación de archivos de instalación del software							2	2	**10**	TT

		Acceso al software por usuarios no autorizados							2	2	**10**	TT
12	Motores de Base de Datos -MySQL -DB2 -Access	Mala instalación, configuración, actualización de software	**3**	**4**	**4**	**11**	- No existe con manuales de soporte para la solución de problemas (configuraciones, instalaciones y actualizaciones.)	-Obtener backup de la información -Registro de incidente en sistema de Requerimientos por errores que se presentan	2	5	**21**	RT
		Infección por código malicioso, virus, troyanos, gusanos					-No contar con antivirus o que esté desactualizado		1	5	**16**	RT
		Caída de los motores de BD - Impacto en Aplicativos					- No hay ambiente para poder efectuar pruebas por actualización de versión. -Impacto en los sistemas por actualización de versión		2	5	**21**	RT
		Falta de soporte técnico apropiado para los software					- Desconocimiento del personal de soporte para la solución de problemas (configuraciones y actualizaciones.)		2	5	**21**	RT
		Accesos al software por usuarios no autorizados					- No se cuenta con el control de accesos configurado por usuario		2	5	**21**	RT
		Herramientas desactualizadas / no vigentes					-No se cuenta con el soporte para actualizar herramientas		2	3	**17**	RT
		Cambio de versión de las herramientas y entornos					-No se cuenta con un soporte para revisar el cambio de versión		2	4	**19**	RT
		Instalación de software no licenciados					-No se cuenta con un control para instalación de software no licenciado		2	5	**21**	RT
		Falta de renovación de licencias.					- El amarre de los desarrollos a las versiones del software.		2	5	**21**	RT
		Falta de licencias para el software					- Número limitado de licencias para los software		2	3	**17**	RT

		Eliminación de archivos propios del lenguaje					- Desconocimiento del personal de soporte para la solución de problemas (configuraciones y actualizaciones.)		2	3	**17**	RT
13	-Herramientas para Gestión de Proyectos -Open Project -MS Project	Mala instalación del software	**1**	**1**	**4**	**6**	-Número limitado de licencias para el MS Project. - Desarrolladores no cuentan con visores confiables para MS Project.	-Registro de Aranda por errores que se presentan	2	2	**10**	TT
		Infección por código malicioso, virus, troyanos, gusanos							3	1	**9**	TT
		Falta de soporte técnico apropiado para el software							3	1	**9**	TT
		Modificación de la configuración por efecto utilizado por el software							3	1	**9**	TT
		Eliminación de archivos de instalación del software							2	2	**10**	TT
		Acceso al software por usuarios no autorizados							3	1	**9**	TT
14	PC Virtuales	Mal rendimiento de las PCs Virtuales	**1**	**2**	**3**	**6**	-Capacidad de los equipos para trabajar con PC's Virtuales	-Registro de Aranda por errores que se presentan	2	3	**12**	TT
15	Aplicativos en Servidor AS/400	Mala instalación de los aplicativos	**2**	**4**	**4**	**10**	- Desconocimiento en la instalación de los sistemas por parte del personal de Soporte Técnicos.	-Definición de accesos en base a perfil de usuario -Registro de incidente en sistema de Requerimientos por errores que se presentan	3	3	**19**	RT
		Cambios de versión en los software base					-No se cuenta con adecuado control de cambios		3	3	**19**	RT
		Difícil entendimiento de la funcionalidad de los aplicativos por parte del equipo de desarrollo					- Falta de documentación técnica de desarrollos existente.		3	3	**19**	RT
		Desarrollos fuera del estándar de programación					- No se difunde e indica con claridad que estándares utilizar		3	3	**19**	RT

		Estándares de programación desactualizados					- No se actualizan los estándares utilizadas para el desarrollo de aplicativos		2	3	**16**	RT
		Pérdida parcial /total de los códigos fuente					- No se cuenta con un control de versiones de los sistemas desarrollados.		3	5	**25**	RT
		Paralización en la atención de desarrollos de proyectos y requerimientos por activación de la contingencia					- No existe servidores de contingencia para los servidores de desarrollo - Ambiente de pruebas y desarrollo es el mismo servidor		3	5	**25**	RT
		Accesos no autorizados					- No se cuenta con un inventario actualizado de los sistemas y de los usuarios por cada uno de ellos.		3	5	**25**	RT
		Inyección de código malicioso					-No contar con antivirus o que esté desactualizado		2	5	**20**	RT
		Pase producción desde ambiente de desarrollo.					- No realiza el control de cambios adecuado para que los aplicativos desarrollados pasen primero por certificación		4	5	**30**	NT
		Modificación/Eliminación/Robo de información					- No se cuenta con un Control adecuado sobre el acceso del código fuente. - No se cuenta con métodos de encriptación		4	5	**30**	NT
16	Aplicativos Visual Basic Aplicativos .NET	Mala instalación de los Aplicativos	**2**	**4**	**4**	**10**	- Desconocimiento en la instalación de los sistemas por parte del personal de Soporte Técnicos.	-Definición de accesos en base a perfil de usuario -Registro de incidente en sistema de Requerimientos por errores que se presentan	3	3	**19**	RT
		Cambios de versión en los software base					-No se cuenta con adecuado control de cambios		3	3	**19**	RT
		Difícil entendimiento de la funcionalidad de los Aplicativos por parte del equipo de desarrollo					- Falta de documentación técnica de desarrollos existente.		3	3	**19**	RT

		Desarrollos fuera del estándar de programación					- No se difunde e indica con claridad que estándares utilizar		3	3	**19**	**RT**
		Pérdida parcial /total de los códigos fuente					- No se cuenta con un control de versiones de los sistemas desarrollados.		3	5	**25**	**RT**
		Paralización en la atención de desarrollos de proyectos y requerimientos por activación de la contingencia.					- No existe servidores de contingencia para los servidores de desarrollo - Ambiente de pruebas y desarrollo es el mismo servidor		3	5	**25**	**RT**
		Inyección de código malicioso					-No contar con antivirus o que esté desactualizado		2	5	**20**	**RT**
		Accesos no autorizados					- No se cuenta con un inventario actualizado de los sistemas y de los usuarios por cada uno de ellos.		3	5	**25**	**RT**
		Software de desarrollo Visual Basic desactualizado y sin soporte					- Existencia de aplicativos para funcionalidades especificas no integradas a un sistema principal.		4	3	**22**	**RT**
		Pase producción desde ambiente de desarrollo.					- No se cuenta con un Control adecuado sobre el acceso del código fuente. - No se cuenta con métodos de encriptación		4	5	**30**	**NT**
17	Aplicativos JAVA	Instalación incorrecta de los Aplicativos	**2**	**4**	**4**	**10**	- Desconocimiento en la instalación de los sistemas por parte del personal de Soporte Técnicos.	-Definición de accesos en base a perfil de usuario -Registro de incidente en sistema de Requerimientos por errores que se presentan	3	3	**19**	**RT**
		Cambios de versión en los software base					-No se cuenta con adecuado control de cambios		3	3	**19**	**RT**

		Paralización en la atención de desarrollos de proyectos y requerimientos por activación de la contingencia.					- No existe servidores de contingencia para los servidores de desarrollo - Ambiente de pruebas y desarrollo es el mismo servidor		3	5	**25**	**RT**
		Inyección de código malicioso					-No contar con antivirus o que esté desactualizado		2	5	**20**	**RT**
		Pase producción desde ambiente de desarrollo.					- No realiza el control de cambios adecuado para que los aplicativos desarrollados pasen primero por certificación		4	5	**30**	**NT**
19	Desarrollos Terciarizados	Retrasos / errores en la implementación de desarrollos terciarizados	**3**	**4**	**4**	**11**	- No existe metodología de desarrollo con terceros.	-Definición de accesos en base a perfil de usuario -Registro de incidente en sistema de Requerimientos por errores que se presentan	2	4	**19**	**RT**
		Difícil entendimiento de los Aplicativos					- Falta de documentación técnica de desarrollos existente		2	4	**19**	**RT**
		Divulgación / Modificación / Eliminación de información					- No se cuenta con un Control adecuado sobre el acceso del código fuente y la información de la BD		3	4	**23**	**RT**
		Incumplimiento de contratos con terceros					- No se cuenta con un contrato modelo para tercerización de desarrollo de software.		3	5	**26**	**NT**
20	Cristal Report	Mala instalación del software	**1**	**2**	**3**	**6**	- Falta de revisión para las actualizaciones de software - No se cuenta con documentación de instalación y configuraciones. - Licencias limitadas	-Registro de Aranda por errores que se presentan	1	1	**7**	**TT**
		Infección por código malicioso, virus, troyanos, gusanos							2	1	**8**	**TT**
		Falta de soporte técnico apropiado para el software							3	1	**9**	**TT**
		Modificación de la configuración por efecto utilizado por el software							2	2	**10**	**TT**
		Eliminación de archivos de instalación del software							2	2	**10**	**TT**

		Acceso al software por usuarios no autorizados							1	1	**7**	**TT**
21	Ms Acces	Mala instalación del software	**1**	**3**	**3**	**7**	-No existe uniformidad en las versiones. -Impacto en los sistemas por actualización de versión	-Registro de Aranda por errores que se presentan	1	1	**8**	**TT**
		Infección por código malicioso, virus, troyanos, gusanos							2	1	**9**	**TT**
		Falta de soporte técnico apropiado para el software							2	1	**9**	**TT**
		Modificación de la configuración por efecto utilizado por el software							1	2	**9**	**TT**
		Eliminación de archivos de instalación del software							1	2	**9**	**TT**
		Acceso al software por usuarios no autorizados							1	1	**8**	**TT**

			¿Qué afecta?						Riesgo Efectivo			
Nro.	**ACTIVOS AFECTADOS**	**AMENAZA**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valoración**	**VULNERABILIDADES**	**Mecanismos de protección existentes**	**Probabilidad**	**Impacto**	**Riesgo**	**Tolerancia**
RIESGOS A LOS ACTIVOS DE SERVICIOS												
22	**Servicios en Línea** Procesos MC (POS) Global NET (ATM) Pulse (ATM) DCISC (POS) Banco Financiero (D.	Cambios en la estructura de tramas de envió y repuestas	3	3	4	**10**	- No existe una comunicación oportuna por cambio en las estructura de tramas	-Registro de incidencia en Sistema de Requerimientos por errores que se presentan	2	4	**18**	**RT**
		Recursos con poca experiencia y conocimientos en tema de comunicaciones.					- Falta de capacitación para el personal		3	3	**19**	**RT**

	Efectivo) Dad (SMS - Mail) Web Service Travel Account	Modificación/Eliminación de información por entes externos					- No se cuenta con una línea segura para realizar el intercambio de información con terceros		2	4	**18**	**RT**
		Retraso en establecimiento de ambiente de pruebas					- No existe un procedimiento difundido para establecer los ambientes de prueba/certificación entre CP y Procesos MC.		2	4	**18**	**RT**
23	**Servicios en Lotes** Procesos MC Global Net DCISC (Xchange, Settlement) Banco Financiero IATA Recaudación Bancos CAD TACA Coris Courier (Urbano) Web Service PNR - Empresas Verificadoras Venta de Cartera de Bancos Central de Riesgos	Cambios en la estructura de tramas de envió y repuestas	3	3	4	**10**	- No existe una comunicación oportuna por cambio en las estructura de tramas	-Registro de incidencia en Sistema de Requerimientos por errores que se presentan	2	4	**18**	**RT**
		Recursos con poca experiencia y conocimientos en tema de comunicaciones.					- Falta de capacitación para el personal		2	4	**18**	**RT**
		Implementación de procesos batcheros en momentos no adecuados					- No se cuenta con una línea segura para realizar el intercambio de información con terceros		3	3	**19**	**RT**
		Retraso en establecimiento de ambiente de pruebas					- No existe un procedimiento difundido para establecer los ambientes de prueba/certificación entre CP y Procesos MC.		2	4	**18**	**RT**
24	Servicio Data Crédito	Retraso en establecimiento de ambiente de pruebas	2	2	2	**6**	No existe un procedimiento difundido para establecer los ambientes de prueba / certificación entre CP y Data Crédito	-Registro de Aranda por errores que se presentan	2	2	**10**	**TT**
25	- Servicio cobranza: Tec Center y Pague Ya	Retraso en establecimiento de ambiente de pruebas	2	1	3	**6**	- No existe un procedimiento difundido para establecer los	-Registro de Aranda por errores que se presentan	2	2	**10**	**TT**

	- Servicio Infocor - Servicio Certicon	Modificación/Eliminación de información por entes externos					ambientes de prueba - No tenemos una línea segura para el intercambio de información		2	2	**10**	**TT**
26	DCI: Global Vision	Retraso en el envío de información de respuesta ante errores reportados.	2	1	3	**6**	- No se cuenta con una área responsable de la información y control de la información enviada - No se cuenta con más de una persona que sepa del sistema de Global Visión - Se desconoce el flujo de comunicación ante un error reportado por DCI - No existe un procedimiento difundido para establecer los ambientes de prueba	-Registro de Aranda por errores que se presentan -Registro de Incidencia en sistema de Requerimientos	2	2	**10**	**TT**
		Retraso en establecimiento de ambiente de pruebas							2	2	**10**	**TT**
27	DCI: Consumos Internacionales - facturación	Retraso en el envío de información de respuesta ante errores reportados.	2	1	3	**6**	- Se desconoce el flujo de comunicación ante un error reportado por DCI. - No existe un procedimiento difundido para establecer los ambientes de prueba	-Registro de Aranda por errores que se presentan -Registro de Incidencia en sistema de Requerimientos	2	2	**10**	**TT**
		Retraso en establecimiento de ambiente de pruebas							2	2	**10**	**TT**
28	Urbano	Retraso en el cumplimiento de los envíos	2	1	3	**6**	-No contar con un contrato bien definido en caso de incumplimiento		2	2	**10**	**TT**
29	Central Crediticia RCC	Retraso en establecimiento de ambiente de pruebas	2	2	2	**6**	- No existe un procedimiento difundido para establecer los ambientes de prueba	-Registro de Aranda por errores que se presentan	2	1	**8**	**TT**

			¿Qué afecta?						Riesgo Efectivo			
Nro.	ACTIVOS AFECTADOS	AMENAZA	Confidencialidad	Integridad	Disponibilidad	Valoración	VULNERABILIDADES	Mecanismos de protección existentes	Probabilidad	Impacto	Riesgo	Tolerancia
COLABORADORES CP												
30	Analista Programador Sr. Analista Programador Arquitecto Analista de Calidad Programador Sr. Programador Jr. Jefe Proyecto Jefe de Desarrollo Practicante de Desarrollo	Indisponibilidad del personal	3	3	3	9	- No existe políticas y procedimientos - Desconocimiento de las funciones y responsabilidades inherentes al cargo	-Política y procedimiento de selección de nuevo personal	2	4	17	RT
		Poco interés del personal en seguridad de información					- No existe una cultura de Seguridad de información		2	4	17	RT
		Robo de información					- Nivel de compromiso del colaborador con la empresa.		2	4	17	RT
		Extorsión					-No existe un seguro de protección contra Extorsión		1	1	10	TT
31	Personal Externo (subcontratado, outsourcing)	Indisponibilidad del personal	2	3	2	7	-No se cuenta con niveles de acceso a la información para terceros -Se desconoce si existe política de firma de acuerdos de confidencialidad		1	1	8	TT
		Grado de rotación del personal							2	1	9	TT
		Extorsión							2	1	9	TT

b) Análisis y evaluación de riesgos: Business intelligence

Nro.	ACTIVOS AFECTADOS	AMENAZA	¿Qué afecta?				VULNERABILIDADES	Mecanismos de protección existentes	Riesgo Efectivo			
			Confidencialidad	Integridad	Disponibilidad	Valoración			Probabilidad	Impacto	Riesgo	Tolerancia
RIESGOS DE LOS ACTIVOS DE INFORMACION												
1	-Documentación (Actas, avances) - Documentos de Análisis - Documentos de Diseño - Documentos de Despliegue - Documentación de Proyecto - Procedimientos de Negocio - Documentos de Análisis e Investigación	Fuga/Divulgación de información por parte del personal interno	**3**	**3**	**3**	**9**	- No existe políticas, cartas u otros documentos que evidencien confidencialidad de información.	- Backup - Permisos adecuados - Verificación antes de su uso - Revisión paso a paso	2	4	**17**	RT
		Modificación de información - accidental					-No se cuenta con el control de accesos configurado por usuario. -No se cuenta con Sistema de control de cambios/versiones.		2	4	**17**	RT
		Información desactualizada / No disponible					-No contar un procedimiento para actualización de información		2	4	**17**	RT
		Robo de Documentos de proyectos					- Los documentos son fácilmente extraíbles		2	4	**17**	RT
		Accesos no autorizados					- No se cuenta con el control de accesos configurado por usuario.		2	4	**17**	RT
2	Bases de Datos Externas	Fuga/Divulgación de información por parte del personal interno	**3**	**3**	**4**	**10**	- No existe políticas, cartas u otros documentos que evidencien confidencialidad de información.	- Entrenamiento de personal - Selección de proveedores confiables - Permisos adecuados	2	5	**20**	RT

		Modificación de información - accidental / Intencional					- No se tienen definidos los accesos	- Consultar errores frecuentes - Corrección	3	5	**25**	RT
		Robos de Base de datos					- Los documentos son fácilmente extraíbles		2	3	**16**	RT
		Datos inconsistentes					-No se cuenta con un control de ingreso de datos		1	1	**11**	TT
3	-Datawarehouse_DC -Datawarehouse_DT -BDExt - BD Prospectos -BDRCC - BSC	Fuga/Divulgación de información por parte del personal interno	**5**	**5**	**5**	**15**	- No existe políticas, cartas u otros documentos que evidencien confidencialidad de información.	- Antivirus actualizado - Consultar y editar en entorno de Desarrollo - Permisos adecuados - Verificación antes de su uso - Backup - Antivirus - Alertas por error de procesamiento - Actualización y eliminación con antivirus - Restauración de Backup	2	5	**25**	RT
		Modificación de información - accidental / Intencional					- No se cuenta con perfiles de acceso personalizado.		3	5	**30**	NT
		Interrupción del servicio de Base de Datos					- Problemas constantes en los servidores		2	3	**21**	RT
		Virus, troyanos, gusanos especializados que afecten específicamente bases de datos					-No contar con antivirus o que esté desactualizado		1	4	**19**	RT
		Sobrecarga de Procesamientos					- No se realiza controles para validación del procesamiento de información		2	4	**23**	RT
		Daño/Corrupción de la Base de Datos					- Equipos de producción y desarrollo/pruebas en un mismo ambiente físico.		2	4	**23**	RT
		Accesos no autorizados					- No se cuenta con perfiles de acceso personalizado.		3	4	**27**	NT
		Pérdida parcial o completa de información					-No contar con backup		1	4	**19**	RT
4	Indicadores BI Dashboard BSC	Fuga/Divulgación de información por parte del personal interno	**2**	**2**	**1**	**5**	- No existe políticas, cartas u otros documentos que evidencien confidencialidad de información.	- Backup - Permisos adecuados - Editar en entorno de Desarrollo - Verificación antes de su uso - Observaciones de usuarios. - Seguimiento - Corrección y	2	2	**9**	TT
		Indicadores Inconsistentes					- No se tienen definidos los accesos		1	4	**9**	TT
		Caída de Servicio de Reportería					- Los documentos son		1	4	**9**	TT

							fácilmente extraíbles	actualización				
		Pérdida parcial o completa de información					-No se cuenta con un control de ingreso de datos		1	4	**9**	TT
RIESGOS DE LOS ACTIVOS DE SOFTWARE												
5	Access Erwin Excel Live Office MS Office Xcelsius 2008 Outlook SAP Business Object SQL Server 2008	Mala instalación del software	**3**	**3**	**2**	**8**	- Falta de soporte técnico apropiado para el software		2	3	**14**	TT
		Herramientas desactualizadas / no vigentes					-No se cuenta con el soporte para actualizar herramientas		2	3	**14**	TT
		Instalación de software no licenciados					-No se cuenta con un control para instalación de software no licenciado		2	5	**18**	RT
		Falta de renovación de licencias.					- El amarre de los desarrollos a las versiones del software.		2	5	**18**	RT
		Infección por código malicioso, virus, troyanos, gusanos					-No contar con antivirus o que esté desactualizado		1	3	**11**	TT
		Modificación de la configuración utilizado por el software					-No contar con un control para lo modificación de configuraciones		1	3	**11**	TT
		Falta de licencia para el software					- Poco stock de licencias		2	3	**14**	TT
		Corrupción de archivos					- No se conoce los tiempos de Back UP		2	3	**14**	TT
7	Infoview	Mala instalación del software	**2**	**2**	**2**	**6**	- Corrupción de reportes		2	2	**10**	TT
		Infección por código malicioso, virus, troyanos, gusanos							2	2	**10**	TT
		Falta de soporte técnico apropiado para el software							2	2	**10**	TT
		Modificación de la configuración por efecto utilizado por el software							2	2	**10**	TT
		Falta de licencia para el software							1	3	**9**	TT

		Eliminación de archivos de instalación del software							2	2	**10**	TT
		Acceso al software por usuarios no autorizados							1	3	**9**	TT
8	Programas AS/400 Programas SQL Soluciones Integration Services	Accesos por usuarios no autorizados	**5**	**5**	**5**	**15**	- No se cuenta con un control adecuado sobre el acceso del código fuente.	- Backup	3	3	**24**	RT
		Infección por código malicioso, virus, troyanos, gusanos					-No contar con antivirus o que esté desactualizado		1	3	**18**	RT
		Inyección de código malicioso					-No contar con antivirus o que esté desactualizado		2	4	**23**	RT
		Modificación de información intencional / Accidental					-No existe control de cambios estandarizado SQL. -No se cuenta con ambientes separados de producción y desarrollo (SQL)		3	4	**27**	NT
		Pérdida y/o Corrupción de archivos					-No existe control de cambios estandarizado SQL. -No se cuenta con ambientes separados de producción y desarrollo (SQL)		3	4	**27**	NT
10	Macros	Modificación de información - accidental / Intencional	**3**	**3**	**4**	**10**	- Poca Seguridad para interacción con la base de datos	- Backup - Permisos adecuados - Verificación antes de su uso	3	4	**22**	RT
		Pérdida parcial o completa del Código fuente					- No se cuenta con un control adecuado sobre el acceso del código fuente.		3	4	**22**	RT
COLABORADORES CP												
12	Analista BI Coordinador BI Desarrollador BI	Indisponibilidad del personal	**3**	**5**	**4**	**12**	- No existen políticas y procedimientos - Desconocimiento de las funciones y responsabilidades inherentes al cargo	Se cuenta con documentación estandarizada	2	3	**18**	RT

		Poco interés del personal en seguridad de información					- No existe una cultura de Seguridad de información		2	3	**18**	RT
		Robo de información					- Nivel de compromiso del colaborador con la empresa.		3	2	**18**	RT
		Extorsión					-No existe un seguro de protección contra Extorsión		1	3	**15**	TT
13	Líder de Proyecto Patrocinador de Proyecto Líder Usuario	Indisponibilidad del personal	**1**	**1**	**2**	**4**	-Desconocimiento de la Seguridad a aplicar en concordancia con las políticas y los procedimientos de la empresa. -Desconocimiento de las funciones y responsabilidades inherentes al cargo -Grado de rotación del personal. -Nivel de compromiso del empleado con la empresa. -No existen controles y procedimientos que expliquen como es que el personal debe reportar los incidentes de seguridad de la información.		2	3	**10**	TT
		Mal clima laboral							2	2	**8**	TT
		Robo de información							2	2	**8**	TT
		Extorsión							1	3	**7**	TT

Cuadro 3.20: Análisis y evaluación de riesgos de departamento de business intelligence [54]

[54] Elaboración: los autores.

c) Análisis y evaluación de riesgos: Centro de cómputo

¿Aplica? SI/NO	ACTIVOS AFECTADOS	AMENAZA	¿Qué afecta?				VULNERABILIDADES	Mecanismos de protección existentes	Riesgo Efectivo			
			Confidencialidad	Integridad	Disponibilidad	Valoración			Probabilidad	Impacto	Riesgo	Tolerancia
RIESGOS DE LOS ACTIVOS DE INFORMACIÓN												
1	Bitácora de procesos diarios	Pérdida física de bitácora	2	2	1	5	- Ausencia del personal de Producción		1	2	**10**	**TT**
		Modificación/Eliminación del formato					- Formato de Bitácora editable		3	2	**14**	**TT**
		Mala ejecución de los procesos					- Ausencia de instrucciones técnicos de trabajos		3	3	**17**	**RT**
2	Reportes especies valoradas(facturas, N/C, boletas, cheques, claves)	Daño / Deterioro del papel pre-impreso (polvo, agua, etc.)	1	1	1	3	-No contar con la aclimatación para el papel	-Control de acceso físico - Control de visitantes	2	2	**7**	**TT**
		Acceso no autorizado					- Ausencia del personal de Producción		2	2	**7**	**TT**
		Desperfecto en impresión de documentos					- Ausencia del personal de Producción - Ausencia de transferencia de conocimiento		2	2	**7**	**TT**
		Mala impresión de documentos					- Ausencia del personal de Producción - Ausencia de transferencia de conocimiento		2	2	**7**	**TT**
		Pérdida de documentos					- Ausencia del personal de Producción		2	3	**9**	**TT**
3	Reportes cierre diario	Acceso no autorizado	1	1	1	3	- Ausencia del personal de Producción	-Control de acceso físico - Control de visitantes	3	2	**9**	**TT**

		Daño / Deterioro (polvo, agua, etc.)					-No contar con la aclimatación para el papel	-Control de acceso físico - Control de visitantes	3	2	**9**	**TT**
		Eliminación lógica de reportes					- Ausencia del personal de Producción		3	2	**9**	**TT**
		Mala distribución del reporte					- Ausencia de control de reportes		3	2	**9**	**TT**
4	Documentación del proyecto Documentación de prueba Informe del Proyecto Documentación de tecnología Informe de propuesta	Acceso no autorizado	2	2	2	6	- Ausencia del personal de Producción	- Control de acceso lógico por roles	3	2	**12**	**TT**
		Daño / Deterioro (polvo, agua, etc.)					-No contar con la aclimatación para el papel		3	2	**12**	**TT**
		Eliminación lógica de reportes					- Ausencia del personal de Producción		3	2	**12**	**TT**
		Mala distribución del reporte					- Ausencia de control de reportes		3	2	**12**	**TT**
5	Orden de compra	Acceso no autorizado	1	1	1	3	- No se cuenta con control de acceso		3	2	**9**	**TT**
		Daño / Deterioro (polvo, agua, etc.)					- No se cuenta con control de acceso		3	2	**9**	**TT**
		Mala distribución del reporte					- Ausencia de control de reportes		3	2	**9**	**TT**
6	Inventario de HW y SW	Acceso no autorizado	1	1	1	3	- Ausencia del personal de Producción	- Control de acceso lógico por roles	3	2	**9**	**TT**
		Daño / Deterioro (polvo, agua, etc.)					-No contar con la aclimatación para el papel		3	2	**9**	**TT**
		Eliminación lógica de reportes					- Ausencia del personal de Producción		3	2	**9**	**TT**
		Mala distribución del reporte					- Ausencia de control de reportes		3	2	**9**	**TT**
7	Licencia de Tecnología Contratos de Mantenimiento Contratos de Soporte	Pérdidas de los documentos de licencia físicas y ausencia de control de renovaciones.	3	3	3	9	- No se cuenta con inventario de licencias - No se digitalizan las licencias		3	4	**21**	**RT**

		Pérdida de los contratos físicos y ausencia de control de renovaciones.					-No se cuenta con un control de los contratos físicos adecuados		3	4	**21**	**RT**
		Mala interpretación de licencias					---		1	4	**13**	**TT**
		Mal uso de licencias					---		1	4	**13**	**TT**

Cuadro 3.21: Análisis y evaluación de riesgos de departamento de centro de cómputo [55]

			¿Qué afecta?						Riesgo Efectivo			
¿Aplica? SI/NO	**ACTIVOS AFECTADOS**	**AMENAZA**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valoración**	**VULNERABILIDADES**	**Mecanismos de protección existentes**	**Probabilidad**	**Impacto**	**Riesgo**	**Tolerancia**
RIESGOS DE LOS ACTIVOS DE SOFTWARE												
8	**Servidores Virtuales:** Servidor Exchange Servidor de Archivos SYBASE BI BI SQL Card al día EPM Intranet BI Desarrollo	Falla de Equipos	3	3	4	10	- Ausencia de repuestos en stock - Ausencia de garantía - Ausencia de contingencia de servidores - Instalaciones eléctricas inadecuadas - Ausencia de programa de mantenimiento preventivo	Monitoreo de espacio en disco -UPS 1+1 -Grupo electrógeno	2	5	**20**	**RT**
		Falta de espacio en disco					- Ausencia de alertas - Ausencia de solución automatizada		3	5	**25**	**RT**

[55] Elaboración: los autores.

	Servidor de Impresoras Sharepoint	Falla de energía y otras interrupciones eléctricas			- UPS soporta carga de equipos del Dpto. de desarrollo (no dedicado)		2	5	**20**	**RT**
		Virus, troyanos, gusanos especializados que afecten específicamente servidores			- Ausencia de monitoreo del estado del antivirus		3	5	**25**	**RT**
		Mala manipulación de equipos			- Ausencia de instructivos de soporte		3	4	**22**	**RT**
		Falla en Firewall			- Ausencia de dispositivo de respaldo en alta disponibilidad		2	5	**20**	**RT**
		Equipo descontinuado			-No se cuenta con soporte para renovación de equipos		2	3	**16**	**RT**
		Saturación de Rack de servidores			---		1	5	**15**	**TT**
		Sobrecarga de tráfico en red LAN			-No se cuenta con herramientas de tráfico de red		2	5	**20**	**RT**
		Mala configuración			-No se cuenta con personal correctamente capacitado para la configuración		2	4	**18**	**RT**
		Acceso no autorizado			- Ausencia de control de claves - Ausencia de control dual de clave maestra - Mal funcionamiento del sistema de control de accesos de producción. - La puerta del Data Center es de madera - El perímetro del data center no es seguro (Paredes de drywall) - No se cuenta con sistemas de seguridad adecuados		2	5	**20**	**RT**

		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)					- Ausencia de programa de mantenimiento preventivo - No se cuenta con detectores de temperatura - No se cuenta con aire acondicionado especial para Data Center		3	4	**22**	**RT**
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)					- Ausencia de detector de aniego - Ausencia de detector de incendios - Ausencia de contingencia de servidores - Ausencia de extintores de gas de halotron		1	5	**15**	**TT**
		Robo de equipo					- Ausencia de Controles físicos - No se controla acceso físico de los visitantes - No se cuenta con Controles físicos del personal a lugares restringidos		2	5	**20**	**RT**
9	**Base de Datos:** DB2 ORACLE MYSQL SYBASE	Mala manipulación de las Bases de Datos	3	3	4	10	- Ausencia de instrucciones de trabajos técnicos	Monitoreo de espacio en disco	5	5	**35**	**NT**
		Fallas del software					- No existe un plan de actualización de parches del sistema		2	5	**20**	**RT**
		Acceso no autorizado a las BD					- No se realiza monitoreo a las BD - Ausencia de control de claves - Ausencia de control dual de clave maestra		2	5	**20**	**RT**
		Modificación/Eliminación del la información por acceso no autorizado					- No se realiza monitoreo a las BD - Ausencia de control de claves - Ausencia de control dual de clave maestra		5	5	**35**	**NT**

		Performance de la BD					- No existe monitoreo de log del sistema operativo		3	5	**25**	**RT**
		Robo de información de las BD					- No se realiza monitoreo de accesos - No se encripta/enmascara la información de las BD		3	3	**19**	**RT**

			¿Qué afecta?						**Riesgo Efectivo**			
¿Aplica? SI/NO	**ACTIVOS AFECTADOS**	**AMENAZA**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valoración**	**VULNERABILIDADES**	**Mecanismos de protección existentes**	**Probabilidad**	**Impacto**	**Riesgo**	**Tolerancia**
10	**Herramientas:** Aranda Service Desk MS Office Antivirus Kaspersky Netsupport VMWARE Wesphere Aranda Inventory Subversion Filtro Web BarracudaAntispam Symantec Page Device Control Visión	Acceso no autorizado	2	2	3	7	- Ausencia de control de claves - Ausencia de control dual de clave maestra	Monitoreo de espacio en disco	3	5	**22**	**RT**
		Fallas del software					- No existe un plan de actualización de parches del sistema		2	5	**17**	**RT**
		Mala configuración					- Ausencia de instrucciones de trabajos técnicos		2	5	**17**	**RT**
		Desconfiguración de software					- Ausencia de instrucciones de trabajos técnicos		1	2	**9**	**TT**
		Mala manipulación de las herramientas					- Ausencia de procedimientos de gestión de cambios - Ausencia de alertas - Ausencia de solución automatizada		5	5	**32**	**NT**

11	S.O. Windows Server Estándar S.O. Linux Redhat S.O. Unix S.O. OS/2	Infección por Virus, troyanos, gusanos, otros	4	2	4	10	- Ausencia de monitoreo del estado del antivirus		3	5	**25**	**RT**
		Mala configuración					- Ausencia de instrucciones de trabajos técnicos		2	4	**18**	**RT**
		Fallas del software					- No existe un plan de actualización de parches de S.O.		2	5	**20**	**RT**
		Acceso no autorizado					- Ausencia de control de claves - Ausencia de control dual de clave maestra		2	5	**20**	**RT**
	Business Object	Acceso no autorizado	2	2	3	7	- Ausencia de control de claves - Ausencia de control dual de clave maestra		3	5	**22**	**RT**
		Fallas del software					- No existe un plan de actualización de parches del sistema		2	5	**17**	**RT**
		Mala configuración					- Ausencia de instrucciones de trabajos técnicos		2	5	**17**	**RT**
		Desconfiguracion de software					- Ausencia de instrucciones de trabajos técnicos		1	2	**9**	**TT**
		Mala manipulación de las herramientas					- Ausencia de procedimientos de gestión de cambios - Ausencia de alertas - Ausencia de solución automatizada		5	5	**32**	**NT**
	Drupal	Acceso no autorizado	2	2	3	7	- Ausencia de control de claves - Ausencia de control dual de clave maestra		3	5	**22**	**RT**
		Fallas del software					- No existe un plan de actualización de parches del sistema		2	5	**17**	**RT**
		Mala configuración					- Ausencia de instrucciones de trabajos técnicos		2	5	**17**	**RT**

		Desconfiguracion de software					- Ausencia de instrucciones de trabajos técnicos		1	2	**9**	**TT**
		Mala manipulación de las herramientas					- Ausencia de procedimientos de gestión de cambios - Ausencia de alertas - Ausencia de solución automatizada		5	5	**32**	**NT**
	Sistema de Control de Acceso físico	Falla de hardware	2	3	3	8	- Ausencia de repuestos en stock - Ausencia de garantía - Equipo descontinuado		2	4	**16**	**RT**
12	**Aplicativos:** MOC MCR MAG SIAF Sistema de Control de Cambios SPEED CADWEB CPCobranzas (recaudadoras y cartas) Estado cuenta web (generación de pdf's) Bridge (aplicativo recepción y envío de lote a DCI) Emisión de EECC y Doc. Aut. (Generación txt para Urbano) Inforcorp APP Control Lotes Internacional APP Generación de Lotes Internacional Sistema de seguridad visual APP para Activación de tarjetas Disposición de efectivo (Banco Financiero) Global Vision APP GNI	Acceso no autorizado	3	4	4	11	- Ausencia de control de claves - Ausencia de control dual de clave maestra		3	5	**26**	**NT**
		Desinstalación de aplicativos					- Ausencia de directivas seguridad de equipos		3	5	**26**	**NT**
		Errores en el despliegue de la aplicación					- No se controlan los pases a producción		2	4	**19**	**RT**
		Errores en el tratamiento de la información					- Incompleto control de calidad		5	5	**36**	**NT**

¿Aplica? SI/NO	ACTIVOS AFECTADOS	AMENAZA	¿Qué afecta?				VULNERABILIDADES	Mecanismos de protección existentes	Riesgo Efectivo			
			Confidencialidad	Integridad	Disponibilidad	Valoración			Probabilidad	Impacto	Riesgo	Tolerancia
RIESGOS DE LOS ACTIVOS DE HARDWARE												
13	PC/Laptop	Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)	2	3	3	8	- Ausencia de programa de mantenimiento preventivo	- Acceso restringido - Acceso restringido - Cable de seguridad	2	3	**14**	**TT**
		Mala manipulación de equipos					- Ausencia de política de uso de equipos		3	2	**14**	**TT**
		Trabajos de Mantenimiento en oficinas					- Ausencia de repuestos en stock - Ausencia de programa de mantenimiento preventivo - Instalaciones eléctricas inadecuadas		3	2	**14**	**TT**
		Fallas de equipos					- Ausencia de repuestos en stock - Ausencia de garantía		2	3	**14**	**TT**
		Equipo descontinuado					- Ausencia de repuestos en stock - Ausencia de garantía		2	3	**14**	**TT**
		Infección por código malicioso, virus, troyanos, gusanos					- Ausencia de monitoreo del estado del antivirus		2	3	**14**	**TT**
		Desinstalación de aplicativos y sistemas					-No se cuenta con un control para la desinstalación de aplicativos		3	3	**17**	**RT**

		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)					- No se cuenta con extintores adecuados para los equipos - No se cuenta con detectores de aniego		1	5	**13**	**TT**
		Acceso no autorizado					- Ausencia de activación automática de protector de pantalla		5	2	**18**	**RT**
		Existencia de usuarios genéricos					-No se cuenta con una definición clara de roles de usuarios		5	3	**23**	**RT**
		Pérdida de información por baja de equipos					- Ausencia de protector de pantalla		3	1	**11**	**TT**
		Robo de equipo					- No existe un procedimientos estandarizado/Difundido para uso de equipos fuera / dentro de las instalaciones - Ausencia de controles de seguridad de información (Encriptación) - Ausencia de Controles físicos - No se controla acceso físico de los visitantes - No se cuenta con controles físicos del personal a lugares restringidos.		5	3	**23**	**RT**
14	**Servidores:** AS400 Produccion AS400 Desarrollo Directorio Activo Web Produccion Web Desarrollo Linux Producción Linux Desarrollo Avaya HP Bridge	Falla de Equipos	2	3	5	10	- Ausencia de repuestos en stock - Ausencia de garantía - Ausencia de contingencia de servidores - Instalaciones eléctricas inadecuadas - Ausencia de programa de mantenimiento preventivo	Monitoreo de espacio en disco -UPS 1+1 -GRUPO ELECTROGENO -Control de acceso físico - Control de visitantes	2	5	**20**	**RT**
		Falta de espacio en disco					- Ausencia de alertas - Ausencia de solución automatizada	-Control de acceso físico - Control de visitantes	3	5	**25**	**RT**

	CCTV Backup	Falla de energía y otras interrupciones eléctricas				- UPS soporta carga de equipos del Dpto. de desarrollo (no dedicado)			2	5	**20**	**RT**
		Virus, troyanos, gusanos especializados que afecten específicamente servidores				- Ausencia de monitoreo del estado del antivirus			3	5	**25**	**RT**
		Mala manipulación de equipos				- Ausencia de instructivos de soporte			3	4	**22**	**RT**
		Falla en Firewall				- Ausencia de dispositivo de respaldo en alta disponibilidad			2	5	**20**	**RT**
		Equipo descontinuado				-No se cuenta con soporte para renovación de equipos			2	3	**16**	**RT**
		Saturación de Rack de servidores				---			1	5	**15**	**TT**
		Sobrecarga de tráfico en red LAN				-No se cuenta con herramientas de tráfico de red			2	5	**20**	**RT**
		Mala configuración				-No se cuenta con personal correctamente capacitado para la configuración			2	4	**18**	**RT**
		Acceso no autorizado				- Ausencia de control de claves - Ausencia de control dual de clave maestra - Mal funcionamiento del sistema de control de accesos de producción. - La puerta del Data Center es de madera - El perímetro del data center no es seguro (Paredes de drywall) - No se cuenta con sistemas de seguridad adecuados			2	5	**20**	**RT**

		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)					- Ausencia de programa de mantenimiento preventivo - No se cuenta con detectores de temperatura - No se cuenta con aire acondicionado especial para Data Center		3	4	**22**	**RT**
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)					- Ausencia de detector de aniego - Ausencia de detector de incendios - Ausencia de contingencia de servidores - Ausencia de extintores de gas de halotron		1	5	**15**	**TT**
		Robo de equipo					- Ausencia de controles físicos - No se controla acceso físico de los visitantes - No se cuenta con controles físicos del personal a lugares restringidos		2	5	**20**	**RT**
			¿Qué afecta?						**Riesgo Efectivo**			
¿Aplica? SI/NO	**ACTIVOS AFECTADOS**	**AMENAZA**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valoración**	**VULNERABILIDADES**	**Mecanismos de protección existentes**	**Probabilidad**	**Impacto**	**Riesgo**	**Tolerancia**
15	**Host Security Module:** HSM THALES PRODUCCION HSM THALES DESARROLLO HSM ATALLA PRODUCCION	Falla de hardware	2	2	3	7	- Equipos Thales descontinuados - No se cuenta con soporte de desarrollo	-Control de acceso físico - Control de visitantes	3	5	**22**	**RT**
		Desconfiguracion de equipo					- Ausencia de instrucciones de trabajos técnicos		1	5	**12**	**TT**

	HSM ATALLA DESARROLLO	Perdida de llaves maestras					- No se tienen definidos los responsables de custodio de llaves maestras		2	5	**17**	**RT**
		Mala manipulación de equipos					- Ausencia de instrucciones de trabajos técnicos		3	4	**19**	**RT**
		Falla de energía y otras interrupciones eléctricas					-No se cuenta con sistema de respaldo de energía adecuado		2	5	**17**	**RT**
		Acceso no autorizado					- Ausencia de control de claves		2	5	**17**	**RT**
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)					- Ausencia de detector de aniego - Ausencia de detector de incendios - Ausencia de plan de contingencia de servidores - Ausencia de extintores de gas de halotron		2	4	**15**	**TT**
		Robo de equipo					- Ausencia de controles físicos - No se controla acceso físico de los visitantes - No se cuenta con Controles físicos del personal a lugares restringidos		2	5	**17**	**RT**
16	**Central Telefónica:** Nortel Avaya	Falla de energía y otras interrupciones eléctricas	3	3	3	9	---	Baterías/UPS/Grupo Electrógeno Contrato de mantenimiento preventivo Contrato de mantenimiento preventivo	1	5	**14**	**TT**
		Falla de hardware					- Ausencia de contingencia de central telefónica		2	5	**19**	**RT**
		Falla en Firewall					- Ausencia de dispositivo de respaldo en alta disponibilidad		1	5	**14**	**TT**
		Mala manipulación de equipos					-No se cuenta con personal correctamente capacitado para la configuración		3	4	**21**	**RT**
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad,					---		1	5	**14**	**TT**

		insolación)										
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)					- Ausencia de contingencia de central telefónica - Ausencia de detector de aniego - Ausencia de detector de incendios		1	5	**14**	**TT**
		Robo de equipo					- Ausencia de Controles físicos - No se controla acceso físico de los visitantes - No se cuenta con Controles físicos del personal a lugares restringidos. - Los perímetros de seguridad no están definidos		2	5	**19**	**RT**
17	Impresora	Falla de hardware	2	1	2	5	- Ausencia de Programa de mantenimiento preventivo	- Garantía - Mantenimiento de hardware Contrato de mantenimiento preventivo	2	3	**11**	**TT**
		Mala manipulación de equipos					- Ausencia de instrucciones de trabajos técnicos		4	3	**17**	**RT**
		fallas eléctricas					---		2	2	**9**	**TT**
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)					- Monitoreo de mantenimiento preventivo		2	2	**9**	**TT**
18	Teléfono	Robo de equipo	2	3	3	8	- Ausencia de Controles físicos - No se controla acceso físico de los visitantes		3	3	**17**	**RT**
19	Firewall JUNIPER	Falla de hardware	2	2	3	7	-Ausencia de dispositivo de respaldo en alta disponibilidad	-Control de acceso físico - Control de visitantes	1	5	**12**	**TT**

		Mala manipulación de equipos					- Ausencia del personal de Produccion - Ausencia de instrucciones de trabajos técnicos		2	5	**17**	**RT**
		Acceso no autorizado					- Ausencia de control de claves		1	5	**12**	**TT**
		Ataques externos					-Ausencia de sistema detector de intrusos		1	5	**12**	**TT**
20	**Equipos de Comunicaciones:** Routers Switch Patch Panel	Falla de hardware	3	3	4	10	- Ausencia de equipos de respaldo en stock	-Control de acceso físico - Control de visitantes	1	5	**15**	**TT**
		Equipo descontinuado					- Ausencia de repuestos en stock - Ausencia de garantía		3	4	**22**	**RT**
		Falla de energía					-No se cuenta con sistema de respaldo de energía adecuado		2	4	**18**	**RT**
		Robo de equipo					- Ausencia de Controles físicos - Equipos sin protección física - No se controla acceso físico de los visitantes		3	4	**22**	**RT**
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)					- Ausencia de programa de mantenimiento preventivo		2	4	**18**	**RT**
21	Blackberry	Robo de dispositivo	3	3	3	9	---		3	2	**15**	**TT**
		Mala manipulación de equipos					- Ausencia de política de uso de equipos		1	3	**12**	**TT**
		Acceso no autorizado					---		3	2	**15**	**TT**
		Pérdida de información					- Ausencia de política de robo de equipos		3	3	**18**	**RT**
22	DSC 300 Storage	Mala manipulación de equipos	2	2	5	9	- Ausencia del personal de producción - Ausencia de instrucciones de trabajos técnicos	-Control de acceso físico - Control de visitantes	1	4	**13**	**TT**

		Acceso no autorizado					- La puerta del Data Center es de madera - El perímetro del data center no es seguro (Paredes de drywall) - No se cuenta con sistemas de seguridad adecuados		2	5	**19**	**RT**
		Falla de energía y otras interrupciones eléctricas					- No se cuenta con contingencia		2	5	**19**	**RT**
		Falla de hardware					- Ausencia de equipos de respaldo en stock		1	5	**14**	**TT**
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)					- Ausencia de programa de mantenimiento preventivo - No se cuenta con detectores de temperatura - No se cuenta con aire acondicionado especial para Data Center		3	4	**21**	**RT**
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)					- Ausencia de detector de aniego - Ausencia de detector de incendios - Ausencia de contingencia de servidores - Ausencia de extintores de gas de halotron		1	5	**14**	**TT**
23	Cámaras Vigilancia	Manipulación por personal no calificado	2	2	2	6	- Equipos sin protección física	-Control de acceso físico - Control de visitantes	1	3	**9**	**TT**
		Falla de equipos					- Equipo descontinuado		2	2	**10**	**TT**
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)					- Ausencia de programa de mantenimiento preventivo		2	2	**10**	**TT**

24	**Unidades de Almacenamiento:**Unidades de cinta LTO4Unidades de cinta LTO3DLO Back UP	Acceso no autorizado	2	2	2	6	- Mal funcionamiento del sistema de control de accesos de producción.- La puerta del Data Center es de madera- El perímetro del Data Center no es seguro (Paredes de drywall)- no se cuenta con sistemas de Seguridad adecuados	-Control de acceso físico- Control de visitantes	2	5	**16**	**RT**
		Falla de hardware					- Ausencia de equipos de respaldo en stock		1	5	**11**	**TT**
		Desconfiguracion de equipo					---		1	5	**11**	**TT**
		Falla de energía y otras interrupciones eléctricas					-No se cuenta con sistema de respaldo de energía adecuado		2	5	**16**	**RT**
		Robo de equipos					- Ausencia de Controles físicos - No se controla acceso físico de los visitantes		3	3	**15**	**TT**
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)					- Ausencia de programa de mantenimiento preventivo		2	4	**14**	**TT**
25	**Otros equipos:** Disco duro externo Triturador de papel Modem Claro Control de Acceso Periféricos	Robo de dispositivo	1	1	1	5	- Ausencia de Controles físicos - No se controla acceso físico de los visitantes - Inventario desactualizado		2	2	**9**	**TT**
		Pérdida de información					- Ausencia de pruebas de restauración		5	3	**20**	**RT**
		Infección por código malicioso, virus, troyanos, gusanos					- Ausencia de monitoreo del estado del antivirus		5	2	**15**	**TT**

26	UPS	Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)	3	3	4	10	- Ausencia de programa de mantenimiento preventivo - No se cuenta con detectores de temperatura - No se cuenta con aire acondicionado especial para Data Center	- Contrato de hardware - Contrato de mantenimiento -UPS 1+1 -GRUPO ELECTROGENO	3	4	**22**	**RT**
		Fallas de Equipos					---		1	5	**15**	**TT**
		Equipo descontinuado					- Ausencia de repuestos en stock - Ausencia de garantía		2	3	**16**	**RT**
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)					- Ausencia de detector de aniego - Ausencia de detector de incendios - Ausencia de extintores de gas de halotron		1	5	**15**	**TT**
27	RACK	Fallas de Equipos	1	1	1	3	- Equipos descontinuados		1	5	**8**	**TT**
28	Unidad de cinta	Robo de unidades de cinta	2	2	3	7	- Ausencia de Controles físicos - No se controla acceso físico de los visitantes	- Contrato de Custodia - HERMES -Control de acceso físico - Control de visitantes - Contrato de mantenimiento	3	3	**16**	**RT**
		Pérdida de información					- Ausencia de pruebas de restauración		2	3	**13**	**TT**
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)					- Almacenamiento inadecuado		1	5	**12**	**TT**

¿Aplica? SI/NO	ACTIVOS AFECTADOS	AMENAZA	¿Qué afecta? Confidencialidad	Integridad	Disponibilidad	Valoración	VULNERABILIDADES	Mecanismos de protección existentes	Riesgo Efectivo Probabilidad	Impacto	Riesgo	Tolerancia
RIESGOS A LOS ACTIVOS DE SERVICIOS												
29	**Servicios en Línea** Procesos MC (POS) Global NET (ATM) Pulse (ATM) DCISC (POS) Banco Financiero (D. Efectivo) Web Service movistar (DAD) Web Service Travel Account Bancared Internet CLARO Reniec Hermes Central de Riesgos	Falla en Firewall	2	2	3	7	- Ausencia de servicio de Internet para contingencia	Replicador internet por USB	1	5	**12**	**TT**
		Caída de servicio de internet							1	5	**12**	**TT**
		Ataque externo					-No se cuenta con sistema de detección de intrusos		2	5	**17**	**RT**
		Indisponibilidad de los servicios					- Ausencia de dispositivo de respaldo en alta disponibilidad		2	5	**17**	**RT**
		Sobrecarga de tráfico en red LAN					- Ausencia de sistema detector de intrusos		2	2	**11**	**TT**
30	Central Telefónica AVAYA	Sobrecarga de tráfico en red LAN	2	2	4	8	-No se cuenta con herramientas de tráfico de red		2	5	**18**	**RT**
31	Trafic view	Falla de pagina web	1	2	1	4	- Ausencia de control de tráfico de Internet/Sedes		1	2	**6**	**TT**

		Acceso no autorizado					- Ausencia de control de tráfico de Internet/Sedes		1	2	**6**	**TT**
32	Telebanking (Scotiacargos)	Falla en Firewall	2	2	2	6	-Ausencia de dispositivo de respaldo en alta disponibilidad		1	5	**11**	**TT**
		Sobrecarga de tráfico en red LAN					-No se cuenta con herramientas de tráfico de red		2	2	**10**	**TT**
33	Teletransfer (BCP)	Falla en Firewall	2	2	2	6	- Ausencia de dispositivo de respaldo en alta disponibilidad		1	5	**11**	**TT**
		Sobrecarga de tráfico en red LAN					- No se cuenta con herramientas de tráfico de red		2	2	**10**	**TT**
34	Hermes custodia de medios magnéticos	Pérdida parcial o completa de información	1	2	1	4			1	5	**9**	**TT**
		Robo de información							1	5	**9**	**TT**
		Asalto							1	5	**9**	**TT**
35	Tarjeta Token (BCP)	Falla de dispositivo	1	1	2	4		-Control de acceso físico - Control de visitantes	2	2	**8**	**TT**
		Perdida de dispositivo							2	2	**8**	**TT**
		Robo de dispositivo							2	2	**8**	**TT**
36	**Servicios FTP (terceros) :** Banco Financiero Urbano Procesos MC Data Crédito Ocasa SMP Pulse Supermercados Peruanos	Falla en Firewall	2	2	2	6	-Ausencia de dispositivo de respaldo en alta disponibilidad		1	5	**11**	**TT**
		Sobrecarga de tráfico en red LAN					-No se cuenta con herramientas de tráfico de red		2	2	**10**	**TT**
		Perdida de usuario/clave					- Ausencia de control de claves		2	5	**16**	**RT**
37	**Servicios en Lotes** Procesos MC	Mala ejecución de los procesos	2	2	2	6	-Ausencia de dispositivo de respaldo en alta disponibilidad		3	4	**18**	**RT**
		Archivos recibidos erróneos					---		2	3	**12**	**TT**

	Global Net DCISC (Xchange, Settlement) Banco Financiero IATA Recaudación Bancos CAD TACA Coris Courier (Urbano) Web Service PNR Empresas Verificadoras Venta de Cartera de Bancos Central de Riesgos	Indisponibilidad de los servicios					- Ausencia de dispositivo de respaldo en alta disponibilidad		2	3	**12**	**TT**
		Manipulación de la información					---		2	3	**12**	**TT**
		Caída de servicio de internet					- Ausencia de servicio de Internet para contingencia		2	3	**12**	**TT**
		Falla en Firewall					- Ausencia de dispositivo de respaldo en alta disponibilidad		1	5	**11**	**TT**
38	WEB IATA	Falla en Firewall	2	2	2	6	-Ausencia de dispositivo de respaldo en alta disponibilidad		2	5	**16**	**RT**
		Sobrecarga de tráfico en red LAN					-No se cuenta con herramientas de tráfico de red		2	2	**10**	**TT**
		Acceso no autorizado					- Ausencia de control de claves		1	5	**11**	**TT**
RIESGOS DEL PERSONAL												
39	Personal Card Perú	Indisponibilidad del personal	2	2	3	7	- No existe políticas y procedimientos - Desconocimiento de las funciones y responsabilidades inherentes al cargo		3	3	**16**	**RT**
		Carencia de conocimiento en tecnologías o herramientas implementadas					- No existe una cultura de Seguridad de información		2	3	**13**	**TT**
		Ausencia de cultura en seguridad de la información					-No existen políticas de Seguridad de la información		2	3	**13**	**TT**
		Robo de información					- Nivel de compromiso del colaborador con la empresa.		3	2	**13**	**TT**
		Extorsión					---		1	3	**10**	**TT**

E) Gestión del riesgo

a) Gestión del riesgo: Desarrollo

N°	ACTIVOS DE INFORMACIÓN	AMENAZA	VALORACIÓN	RIESGO EFECTIVO				MECANISMOS DE PROTECCION PROPUESTOS / CONTROLES	TIPO DE CONTROL	COSTO APROX.	TIEMPO APROX.	RIESGO RESIDUAL			TOLERANCIA	RESPONSABLE
				PROBABILIDAD	IMPACTO	RIESGO	TOLERANCIA					PROBABILIDAD	IMPACTO	RIESGO		
1	Documentación Atención al cliente (RQ): -Asignación -Desarrollo -Despliegue	Fuga/Divulgación de información por parte del personal interno	9	2	4	17	RT	* Implementar una política de confidencialidad * Implementar un Compromiso de Confidencialidad Firmado	Reducir	1	C	1	3	12	TT	JD
		Ejecución errónea del proceso de RQ por el usuario y personal de Desarrollo		2	4	17	RT	* Formalizar la metodología de Atención de RQ * Capacitar / Concientizar a los usuarios	Reducir	1	C	1	3	12	TT	JD
		Accesos no autorizados		2	4	17	RT	* Configurar accesos a carpetas por perfiles	Reducir	1	C	1	3	12	TT	JD
		Robo de documentación		2	4	17	RT	* Implementar controles para protección de documentos	Reducir	1	C	1	3	12	TT	JD
		Información desactualizada / No disponible		2	4	17	RT	* Revisiones periódicas del Jefe de Desarrollo.	Reducir	1	C	1	3	12	TT	JD

		Modificación de información - Accidental / Intencional Pérdida parcial / Completa de información		3	4	**21**	**RT**	* Implementar un sistema de control de versiones	Reducir	1	C	1	3	**12**	**TT**	**JD**
2	Documentación Desarrollo de Soluciones: - Análisis - Diseño - Desarrollo - Pruebas - Despliegue	Fuga/Divulgación de información por parte del personal interno	**9**	3	4	**21**	**RT**	* Implementar una política de confidencialidad * Implementar un Compromiso de Confidencialidad Firmado	Reducir	1	C	2	3	**15**	**TT**	**JD**
		Ejecución errónea del proceso por el usuario y personal de Desarrollo		2	5	**19**	**RT**	* Formalizar la metodología de Ingeniería de Software * Capacitar / Concientizar a loa usuarios	Reducir	1	C	1	3	**12**	**TT**	**JD**
		Accesos no autorizados		4	5	**29**	**NT**	* Configurar accesos a carpetas por perfiles	Reducir	1	C	2	4	**17**	**RT**	**JD**
		Información desactualizada / No disponible		2	4	**17**	**RT**	* Revisiones periódicas del Jefe de Desarrollo.	Reducir	1	C	2	2	**13**	**TT**	**JD**
		Robo de documentación		4	5	**29**	**NT**	* Implementar controles para protección de documentos	Reducir	1	C	2	4	**17**	**RT**	**JD**
		Error al realizar las pruebas unitarias		2	4	**17**	**RT**	* Estandarizar y difundir métodos de ejecución de pruebas unitarias	Reducir	1	C	1	1	**10**	**TT**	**JD**
		Modificación de información - Accidental / Intencional Pérdida parcial / Completa de información		3	5	**24**	**RT**	* Implementar un sistema de control de versiones	Reducir	1	C	2	3	**15**	**TT**	**JD**

3	Documentación Control de Calidad de soluciones - Iniciación	Fuga/Divulgación de información por parte del personal interno	9	3	4	**21**	RT	* Implementar una política de confidencialidad * Implementar un Compromiso de Confidencialidad Firmado	Reducir	1	C	1	4	**13**	TT TT	**JD**
	- Elaboración	Ejecución errónea del proceso por el usuario		2	4	**17**	RT	* Reforzar el compromiso de las gerencias con la ejecución de las pruebas	Reducir	1	C	1	4	**13**	TT	**JD**
	- Ejecución	Información desactualizada / No disponible		2	4	**17**	RT	* Revisiones periódicas del Jefe de Desarrollo.	Reducir	1	C	1	3	**12**	TT	**JD**
	- Aceptación	Accesos no autorizados		3	5	**24**	RT	* Configurar accesos a carpetas por perfiles	Reducir	1	C	1	2	**11**	TT	**JD**
		Robo de documentación		3	5	**24**	RT	* Implementar controles para protección de documentos	Reducir	1	C	1	2	**11**	TT	**JD**
		Modificación de información - Accidental / Intencional Pérdida parcial / Completa de información		3	5	**24**	RT	* Implementar un sistema de control de versiones	Reducir	1	C	2	2	**13**	TT	**JD**
4	Herramientas y entornos de desarrollo:	Mala instalación, configuración, actualización de software	8	2	3	**14**	TT	* Implementar manuales, videos, tutoriales para los software	Reducir	2	M	1	1	**9**	TT	**JD**
	-.Net	Herramientas desactualizadas / no vigentes		2	3	**14**	TT	* Revisiones periódicas de nuevas actualizaciones.	Reducir	2	M	1	2	**10**	TT	**JD**
	-Drupal	Cambio de versión de las herramientas y entornos		2	4	**16**	RT	* Planificación del cambio de versiones.	Reducir	3	M	1	2	**10**	TT	**JD**

	-Eclipse (Java)	Instalación de software no licenciados		2	5	**18**	**RT**	* Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir	1	C	2	3	**14**	**TT**	**JD**
	-iSeries	Falta de renovación de licencias.		2	5	**18**	**RT**	* Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir	2	M	1	2	**10**	**TT**	**JD**
	-Visual Basic	Falta de licencias para el software		2	3	**14**	**TT**	* Elaborar un plan de dimensionamiento de licencias según las demandas presentes y futuras.	Reducir	2	M	1	2	**10**	**TT**	**JD**
	-RPG	Eliminación de archivos propios del lenguaje		2	3	**14**	**TT**	* Implementar manuales, videos, tutoriales para los software	Reducir	2	M	1	2	**10**	**TT**	**JD**
5	Motores de Base de Datos	Mala instalación, configuración, actualización de software	**11**	2	5	**21**	**RT**	* Implementar manuales, videos, tutoriales para los software	Reducir	2	M	1	3	**14**	**TT**	**JD**
	-MySQL	Infección por código malicioso, virus, troyanos, gusanos		1	5	**16**	**RT**	* Mantener actualizado los antivirus	Reducir	1	C	1	3	**14**	**TT**	**JD**
	-DB2 -Access	Caída de los motores de BD - Impacto en Aplicativos		2	5	**21**	**RT**	* Implementar un laboratorio para las pruebas de cambios de versiones	Reducir	3	M	1	2	**13**	**TT**	**JD**
		Falta de soporte técnico apropiado para los software		2	5	**21**	**RT**	* Implementar manuales, videos, tutoriales para los software * Imprentar alertas para la caída de correos * Implementar monitoreos de performance de las BD	Reducir	2	M	1	2	**13**	**TT**	**JD**

								* Migración de aplicativos críticos de MySQL a Otra BD										
		Accesos al software por usuarios no autorizados		2	5	**21**	**RT**	* Configurar accesos a carpetas por perfiles	Reducir	2	M	1	2	**13**	**TT**	**JD**
		Herramientas desactualizadas / no vigentes		2	3	**17**	**RT**	* Revisiones periódicas de nuevas actualizaciones.	Reducir	1	C	1	2	**13**	**TT**	**JD**
		Cambio de versión de las herramientas y entornos		2	4	**19**	**RT**	* Planificación del cambio de versiones.	Reducir	1	C	1	2	**13**	**TT**	**JD**
		Instalación de software no licenciados		2	5	**21**	**RT**	* Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir	3	M	2	3	**17**	**RT**	**JD**
		Falta de renovación de licencias.		2	5	**21**	**RT**	* Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir	3	M	1	3	**14**	**TT**	**JD**
		Falta de licencias para el software		2	3	**17**	**RT**	* Elaborar un plan de dimensionamiento de licencias según las demandas presentes y futuras. * Administración de Licencias	Reducir	1	C	1	2	**13**	**TT** **TT**	**JD**
		Eliminación de archivos propios del lenguaje		2	3	**17**	**RT**	* Implementar manuales, videos, tutoriales para los software	Reducir	1	C	1	2	**13**	**TT**	**JD**
6	PC Virtuales	Mal rendimiento de las PCs Virtuales	**6**	2	3	**12**	**TT**	* Definir y evaluar capacidades de las máquinas para trabajar con PC virtuales	Reducir	1	C	1	2	**8**	**TT**	**JD**

7	Aplicativos en Servidor AS/400	Mala instalación de los Aplicativos	**10**	3	3	**19**	RT	* Implementar instructivos de instalación	Reducir	1	C	1	2	**12**	TT	**JD**
		Cambios de versión en los software base		3	3	**19**	RT	* Planificación del cambio de versiones.	Reducir	1	C	1	3	**13**	TT	**JD**
		Difícil entendimiento de la funcionalidad de los Aplicativos por parte del equipo de desarrollo		3	3	**19**	RT	* Elaborar documentación técnica de los desarrollos	Reducir	1	C	1	2	**12**	TT	**JD**
		Desarrollos fuera del estándar de programación		3	3	**19**	RT	* Difundir los estándares de programación	Reducir	1	C	1	2	**12**	TT	**JD**
		Estándares de programación desactualizados		2	3	**16**	RT	* Actualizar los estándares de programación	Reducir	1	C	1	2	**12**	TT	**JD**
		Pérdida parcial /total de los códigos fuente		3	5	**25**	RT	* Implementar un sistema de control de versiones	Reducir	3	M	2	3	**16**	RT	**JD**
		Paralización en la atención de desarrollos de proyectos y requerimientos por activación de la contingencia		3	5	**25**	RT	* Separar los ambientes de contingencia, calidad y desarrollo.	Reducir	3	M	2	3	**16**	RT	**JD**
		Accesos no autorizados		3	5	**25**	RT	* Implementar un laboratorio para las pruebas de cambios de versiones	Reducir	3	M	2	3	**16**	RT	**JD**
		Inyección de código malicioso		2	5	**20**	RT	* Auditoría de código fuente	Reducir	2	M	1	4	**14**	TT	**JD**
		Pase producción desde ambiente de desarrollo.		4	5	**30**	NT	* Separar ambientes de certificación.	Reducir	3	M	2	3	**16**	RT	**JD**

								*Actualizar el sistema de control de cambios para el pase a producción desde ambiente de certificación.										
		Modificación/Eliminación/Robo de información		4	5	**30**	**NT**	* Configurar accesos a código fuente por perfiles *Implementar mecanismos de encriptación de información	Reducir	3	M	2	2	**14**	**TT**	**JD**
8	Aplicativos Visual Basic Aplicativos .NET	Mala instalación de los Aplicativos	**10**	3	3	**19**	**RT**	* Implementar instructivos de instalación	Reducir	2	M	1	1	**11**	**TT**	**JD**
		Cambios de versión en los software base		3	3	**19**	**RT**	* Planificación del cambio de versiones.	Reducir	2	M	1	1	**11**	**TT**	**JD**
		Difícil entendimiento de la funcionalidad de los Aplicativos por parte del equipo de desarrollo		3	3	**19**	**RT**	* Elaborar documentación técnica de los desarrollos	Reducir	2	M	1	2	**12**	**TT**	**JD**
		Desarrollos fuera del estándar de programación		3	3	**19**	**RT**	* Difundir los estándares de programación	Reducir	2	M	1	2	**12**	**TT**	**JD**
		Pérdida parcial /total de los códigos fuente		3	5	**25**	**RT**	* Separar los ambientes de contingencia, calidad y desarrollo.	Reducir	3	M	1	3	**13**	**TT**	**JD**
		Paralización en la atención de desarrollos de proyectos y requerimientos por activación de la contingencia.		3	5	**25**	**RT**	* Separar los ambientes de contingencia, calidad y desarrollo.	Reducir	3	M	2	4	**18**	**RT**	**JD**

		Inyección de código malicioso		2	5	**20**	RT	* Auditoría de código fuente	Reducir	2	M	1	3	**13**	TT	**JD**
		Accesos no autorizados		3	5	**25**	RT	* Desarrollar sistema de control de accesos por aplicativo. * Mejorar el proceso de reserva de fuentes.	Reducir	3	M	1	2	**12**	TT	**JD**
		Software de desarrollo Visual Basic desactualizado y sin soporte		4	3	**22**	RT	* Planificar la migración de aplicativos a java.	Reducir	2	M	1	1	**11**	TT	**JD**
		Pase producción desde ambiente de desarrollo.		4	5	**30**	NT	* Separar ambientes de certificación. *Actualizar el sistema de control de cambios para el pase a producción desde ambiente de certificación.	Reducir	3	M	2	2	**14**	TT	**JD**
9	Aplicativos JAVA	Instalación incorrecta de los Aplicativos	**10**	3	3	**19**	RT	* Implementar instructivos de instalación	Reducir	2	M	1	1	**11**	TT	**JD**
		Cambios de versión en los software base		3	3	**19**	RT	* Planificación del cambio de versiones.	Reducir	2	M	2	2	**14**	TT	**JD**
		Paralización en la atención de desarrollos de proyectos y requerimientos por activación de la contingencia.		3	5	**25**	RT	* Separar los ambientes de contingencia, calidad y desarrollo.	Reducir	3	M	1	1	**11**	TT	**JD**
		Inyección de código malicioso		2	5	**20**	RT	* Auditoría de código fuente	Reducir	2	M	1	2	**12**	TT	**JD**

		Pase producción desde ambiente de desarrollo.		4	5	**30**	**NT**	* Separar ambientes de certificación. *Actualizar el sistema de control de cambios para el pase a producción desde ambiente de certificación.	Reducir	3	M	1	3	**13**	**TT**	**JD**
		Modificación / Eliminación de código fuente		3	5	**25**	**RT**	* Mejorar el proceso de reserva y de fuentes.	Reducir	2	M	1	2	**12**	**TT**	**JD**
10	Desarrollos Terciarizados	Retrasos / errores en la implementación de desarrollos terciarizados	**11**	2	4	**19**	**RT**	* Implementar metodología para el desarrollo de aplicativos con terceros	Reducir	2	M	1	2	**13**	**TT**	**JD**
		Difícil entendimiento de los Aplicativos		2	4	**19**	**RT**	* Solicitar el uso de nuestros estándares de programación. * Solicitar entrenamiento en técnicas de programación utilizadas.	Reducir	2	M	1	1	**12**	**TT**	**JD**
		Divulgación / Modificación / Eliminación de información		3	4	**23**	**RT**	* Contrato de confidencialidad con los proveedores * Encriptación de la información de las bases de datos * Personalizar entrega de fuentes a proveedores	Reducir	2	M	1	1	**12**	**TT**	**JD**
		Incumplimiento de contratos con terceros		3	5	**26**	**NT**	* Elaborar contratos modelos para la tercerización de desarrollos	Reducir	3	M	2	3	**17**	**RT**	**JD**

11	**Servicios en Línea** Procesos MC (POS) Global NET (ATM) Pulse (ATM) DCISC (POS) Banco Financiero (D. Efectivo) Dad (SMS - Mail) Web Service Travel Account	Cambios en la estructura de tramas de envió y repuestas	10	2	4	**18**	RT	* Definir canales de comunicación eficiente	Reducir	1	C	1	2	**12**	TT	**JD**
		Recursos con poca experiencia y conocimientos en tema de comunicaciones.		3	3	**19**	RT	* Entrenamiento de personal.	Reducir	2	M	1	2	**12**	TT	**JD**
		Modificación/Eliminación de información por entes externos		2	4	**18**	RT	* Establecer una línea segura para el intercambio de información.	Reducir	1	C	1	2	**12**	TT	**JD**
		Retraso en establecimiento de ambiente de pruebas		2	4	**18**	RT	* Implementar metodología para configurar ambientes de prueba	Reducir	1	C	1	2	**12**	TT	**JD**
12	**Servicios en Lotes** Procesos MC Global Net DCISC (Xchange, Settlement) Banco Financiero IATA Recaudación Bancos CAD TACA Coris Courier Web Service PNR Empresas Verificadoras Venta de Cartera de Bancos Central de Riesgos	Cambios en la estructura de tramas de envió y repuestas	10	2	4	**18**	RT	* Definir canales de comunicación eficiente	Reducir	1	C	1	2	**12**	TT	**JD**
		Recursos con poca experiencia y conocimientos en tema de comunicaciones.		2	4	**18**	RT	* Entrenamiento de personal.	Reducir	1	C	1	1	**11**	TT	**JD**
		Implementación de procesos batcheros en momentos no adecuados		3	3	**19**	RT	* Documentar los procesos productivos * Capacitación al personal * Analizar procesos bacheros previo a la implementación. * Depuración de procesos bacheros no	Reducir	2	C	2	2	**14**	TT	**JD**

								vigentes								
		Retraso en establecimiento de ambiente de pruebas		2	4	**18**	**RT**	* Implementar metodología para configurar ambientes de prueba	Reducir	2	C	1	1	**11**	**TT**	**JD**
13	Analista Programador Sr. Analista Programador Arquitecto Analista de Calidad Programador Sr. Programador Jr. Jefe Proyecto Jefe de Desarrollo Practicante de Desarrollo	Indisponibilidad del personal	**9**	2	4	**17**	**RT**	* Difundir el MOF para cada puesto * Elaborar un plan de inducción técnico por área.	Reducir	1	C	1	2	**11**	**TT**	**JD**
		Poco interés del personal en seguridad de información		2	4	**17**	**RT**	* Concientizar al personal sobre la Seguridad de Información	Reducir	1	C	2	2	**13**	**TT**	**JD**
		Robo de información		2	4	**17**	**RT**	* Implementar compromiso de confidencialidad	Reducir	1	C	2	1	**11**	**TT**	**JD**
		Extorsión		1	1	**10**	**TT**	-	Aceptar			1	1	**10**	**TT**	**JD**

Cuadro 3.22: Gestión de riesgos de departamento de desarrollo [56]

[56] Elaboración: los autores.

b) Gestión del riesgo: Business intelligence

N°	ACTIVOS DE INFORMACIÓN	AMENAZAS	VALORACIÓN	RIESGO EFECTIVO				MECANISMOS DE PROTECCIÓN PROPUESTOS / CONTROLES	TIPO DE CONTROL	COSTO APROX.	TIEMPO APROX.	RIESGO RESIDUAL				RESPONSABLE
				PROBABILIDAD	IMPACTO	RIESGO	TOLERANCIA					PROBABILIDAD	IMPACTO	RIESGO	TOLERANCIA	
1	-Documentación (Actas, avances) -Documentos de Análisis -Documentos de Diseño -Documentos de Despliegue -Documentación de Proyecto -Procedimientos de Negocio -Documentos de Análisis e Investigación de Solución	Fuga/Divulgación de información por parte del personal interno	9	2	4	17	RT	* Implementar compromiso de confidencialidad de infor.	Reducir	1	C	1	4	13	TT	CBI
		Modificación de información - accidental / Intencional		2	4	17	RT	* Definir y configurar el control de accesos por roles para la documentación de proyectos * Implementar inventario de documentos y control de cambios.	Reducir	1	C	1	4	13	TT	CBI
		Información desactualizada / No disponible		2	4	17	RT	* Revisiones periódicas del Coordinador de B.I.	Reducir	1	C	1	4	13	TT	CBI
		Robo de Documentos de proyectos		2	4	17	RT	* Definir e implementar medidas de seguridad a los documentos	Reducir	1	C	1	4	13	TT	CBI
		Accesos no autorizados		2	4	17	RT	* Definir y configurar el control de accesos por roles.	Reducir	1	C	1	4	13	TT	CBI
2	-Bases de Datos Externas	Fuga/Divulgación de información por parte del personal interno	10	2	5	20	RT	* Implementar compromiso de confidencialidad de infor.	Reducir	2	C	1	5	15	TT	CBI
		Modificación de información - accidental / Intencional		3	5	25	RT	* Definir y configurar el control de accesos por roles para manipulación de bases externas	Reducir	3	M	2	5	20	RT	CBI

		Robos de Base de datos		2	3	**16**	RT	* Definir e implementar medidas de seguridad a los archivos BD	Reducir	1	C	1	3	**13**	TT	CBI
		Datos inconsistentes		1	1	**11**	TT	---	Reducir	1	C	1	1	**11**	TT	CBI
3	- Datawarehouse_DC - Datawarehouse_DT - BDExt - BD Prospectos - BDRCC - BSC	Fuga/Divulgación de información por parte del personal interno	**15**	2	5	**25**	RT	* Implementar compromiso de confidencialidad de infor.	Reducir	3	M	1	4	**19**	RT	CBI
		Modificación de información - accidental / Intencional		3	5	**30**	NT	* Definir y configurar el control de accesos por roles para las bases de datos	Reducir	3	M	1	4	**19**	RT	CBI
		Interrupción del servicio de Base de Datos		2	3	**21**	RT	* Alertas, seguimiento, reportes, etc	Reducir	2	C	1	3	**18**	RT	CBI
		Virus, troyanos, gusanos especializados que afecten específicamente bases de datos		1	4	**19**	RT	* Implementación de antivirus debidamente configurados y actualizados	Reducir	2	C	1	3	**18**	RT	CBI
		Sobrecarga de Procesamientos		2	4	**23**	RT	* Implementar controles de procesamientos de información * Implementar controles de validación de información procesada	Reducir	3	M	2	3	**21**	RT	CBI
		Daño/Corrupción de la Base de Datos		2	4	**23**	RT	* Implementar ambientes de desarrollo diferente al de producción.	Reducir	3	M	1	3	**18**	RT	CBI
		Accesos no autorizados		3	4	**27**	NT	* Definir y configurar el control de accesos por roles para las bases de datos	Reducir	3	M	1	3	**18**	RT	CBI
		Pérdida parcial o completa de información		1	4	**19**	RT	* Backups periódicos de la información	Reducir	2	M	1	3	**18**	RT	CBI
4	- Access - Erwin -Excel - Live Office - MS Office - Xcelsius 2008	Mala instalación del software	**8**	2	3	**14**	TT	* Evaluar y Capacitar al personal responsable para la instalación y configuraciones.	Reducir	1	C	1	3	**11**	TT	CBI
		Herramientas desactualizadas / no vigentes		2	3	**14**	TT	* Revisiones periódicas de nuevas actualizaciones.	Reducir	1	C	1	3	**11**	TT	CBI

	- Outlook - SAP Business Object - SQL Server 2008	Instalación de software no licenciados		2	5	**18**	**RT**	* Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir	1	C	1	5	**13**	**TT**	CBI
		Falta de renovación de licencias.		2	5	**18**	**RT**	* Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir	1	C	1	5	**13**	**TT**	CBI
		Infección por código malicioso, virus, troyanos, gusanos		1	3	**11**	**TT**	---	Reducir	1	C	1	3	**11**	**TT**	CBI
		Modificación de la configuración utilizado por el software		1	3	**11**	**TT**	---	Reducir	1	C	1	3	**11**	**TT**	CBI
		Falta de licencia para el software		2	3	**14**	**TT**	* Elaborar un plan de dimensionamiento de licencias según las demandas presentes y futuras.	Reducir	1	C	1	3	**11**	**TT**	CBI
		Corrupción de archivos		2	3	**14**	**TT**	* Definir tiempos de Back UP	Reducir	1	C	1	3	**11**	**TT**	CBI
5	- Programas as/400 - Programas SQL - S. S. Integration Services	Accesos por usuarios no autorizados	**15**	3	3	**24**	**RT**	* Definir y configurar el control de accesos por roles para el acceso al código fuente de los programas B.I.	Reducir	3	M	1	3	**18**	**RT**	CBI
		Infección por código malicioso, virus, troyanos, gusanos		1	3	**18**	**RT**	---	Reducir	2	C	1	3	**18**	**RT**	CBI
		Inyección de código malicioso		2	4	**23**	**RT**	* Implementar procedimiento para auditoria de fuentes.	Reducir	2	C	1	4	**19**	**RT**	CBI
		Modificación de información intencional / Accidental		3	4	**27**	**NT**	* Implementar ambientes de desarrollo diferente al de producción. * Implementar pases a producción para programas SQL * Se desconoce si se cuenta con historial de cambios realizados. * Implementar inventario de documentos y control de cambios.	Reducir	3	C	1	4	**19**	**RT**	CBI
		Pérdida y/o Corrupción de archivos		3	4	**27**	**NT**		Reducir	3	C	1	4	**19**	**RT**	CBI

6	- Macros	Modificación de información - accidental / Intencional	**10**	3	4	**22**	**RT**	* Desarrollar programas que remplacen las macros	Reducir	2	C	1	4	**14**	**TT**	CBI
		Pérdida parcial o completa del Código fuente		3	4	**22**	**RT**	* Definir y configurar el control de accesos por roles	Reducir	2	C	1	4	**14**	**TT**	CBI
7	- Analista BI - Coordinador BI - Desarrollador BI	Indisponibilidad del personal	**12**	2	3	**18**	**RT**	* Establecer y difundir procedimientos y políticas * Elaborar y difundir MOFs	Reducir	2	C	1	3	**15**	**TT**	CBI
		Poco interés del personal en seguridad de información		2	3	**18**	**RT**	* Concientizar al personal sobre la seguridad de información	Reducir	2	C	1	3	**15**	**TT**	CBI
		Robo de información		3	2	**18**	**RT**	* Implementar compromiso de confidencialidad de infor.	Reducir	2	C	1	2	**14**	**TT**	CBI
		Extorsión		1	3	**15**	**TT**	---	Reducir	1	C	1	3	**14**	**TT**	CBI

Cuadro 3.23: Gestión de riesgos de departamento de business intelligence [57]

[57] Elaboración: los autores.

c) Gestión del riesgo: Centro de cómputo

N°	ACTIVOS DE INFORMACIÓN	AMENAZAS	VALORACIÓN	RIESGO EFECTIVO				MECANISMOS DE PROTECCIÓN PROPUESTOS / CONTROLES	TIPO DE CONTROL	COSTO APROX.	TIEMPO APROX.	RIESGO RESIDUAL				RESPONSABLE
				PROBABILIDAD	IMPACTO	RIESGO	TOLERANCIA					PROBABILIDAD	IMPACTO	RIESGO	TOLERANCIA	
1	PC/Laptop	Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)	8	2	3	**14**	TT	* Implementar programa de mantenimiento preventivo de equipos.	Reducir	1	C	1	3	**11**	TT	JCC
		Mala manipulación de equipos		3	2	**14**	TT	* Capacitación en uso de equipos y seguridad a usuarios CP.	Reducir	1	C	1	2	**10**	TT	JCC
		Trabajos de Mantenimiento en oficinas		3	2	**14**	TT	* Capacitación al equipo de administración en cuidado de equipos * Coordinaciones previas a los trabajos de mantenimiento.	Reducir	1	C	1	2	**10**	TT	JCC
		Fallas de Equipos		2	3	**14**	TT	* Contar con un stock mínimo de repuestos y laptop * Implementar programa de mantenimiento preventivo de equipos. * Corregir las instalaciones eléctricas * Seguimiento a las garantías * Mantener relaciones comerciales con proveedores estratégicos.	Reducir	1	C	1	3	**11**	TT	JCC

		Equipo descontinuado		2	3	**14**	TT	* Establecer un inventario actualizado de equipos (vida útil) * Elaborar plan de renovación de equipos	Reducir	1	C	1	3	**11**	TT	JCC
		Infección por código malicioso, virus, troyanos, gusanos		2	3	**14**	TT	* Implementar informes mensuales sobre estado del antivirus * Habilitar archivo físico para informes mensuales visados. (J. CC)	Reducir	1	C	1	3	**11**	TT	JCC
		Desinstalación de aplicativos y sistemas		3	3	**17**	RT	* Elaborar política de protección de equipo * Habilitar restricciones en el dominio para prohibir desinstalación de programas. * Habilitar el protector de pantalla automático * Habilitar restricciones de eliminación de iconos de escritorio. * Capacitación en seguridad de la información.	Reducir	1	C	1	3	**11**	TT	JCC
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)		1	5	**13**	TT	* Implementar extintores apropiados * Capacitación en uso de extintores * Implementar detectores de aniego * Implementar detectores de fuego	Reducir	2	C	1	4	**12**	TT	JCC
		Acceso no autorizado		5	2	**18**	RT	* Habilitar el protector de pantalla automático * Capacitación en seguridad de la información.	Reducir	1	C	3	2	**14**	TT	JCC
		Existencia de usuarios genéricos		5	3	**23**	RT	* Eliminar usuarios genéricos	Reducir	1	C	3	3	**17**	RT	JCC

		Pérdida de información por baja de equipos		3	1	**11**	**TT**	* Implementar procedimiento de baja de equipos.	Reducir	1	C	2	1	**10**	**TT**	JCC
		Robo de equipo		5	3	**23**	**RT**	* Implementar documentos para el retiro de equipos fuera de las instalaciones (políticas, formatos, procedimientos) * Implementar controles de encriptación de equipos * Implementar controles físicos de seguridad (cables de seguridad para laptops) * Implementar controles para visitas externas * Implementar controles para prevenir el acceso físico del personal a lugares restringidos.	Reducir	3	M	3	3	**17**	**RT**	JCC
2	**Servidores Físicos:** AS400 Producción AS400 Desarrollo Svrdc02 - Directorio Activo BK Svrweb - Web Producción Svrwebpro - Linux Producción Svravaya - Admin. De Central Avaya HP Bridge Svrbkprincipal – Servidor Backup Safeland – CCTV DVR SvrBes – Comunicación Black Berry Svrsmg - Antispan Barracuda - Filtro Web PageControl – Control	Falla de equipos	10	2	5	**20**	**RT**	* Implementar programa de mantenimiento preventivo de equipos. * Implementar mecanismos de control a los contratos de mantenimiento con terceros. * Implementar contingencia de servidores. * Independizar UPS para protección exclusiva de los equipos de C. Cómputo. * Seguimiento a las garantías * Mantener relaciones comerciales con proveedores estratégicos.	Reducir	3	M	1	5	**15**	**TT**	JCC
		Falta de espacio en disco		3	5	**25**	**RT**	* Implementar alertas sobre espacio en disco * Implementar solución automatizada para monitoreo de servidores	Reducir	2	C	1	5	**15**	**TT**	JCC

de impresiones ------ **Servidores Virtuales:** SvrAranda - Aranda service desk/Inventory SvrBisql – MS SQL SvrBides – BI Desarrollo SvrBipro - BI Producción SvrIntranet – IIS Intranet (NO está aún en Producción) SvrKaspersky - Antivirus SvrDc01 – Directorio Activo SvrEpm - cSharepoint SvrFile - Servidor de Archivos SvrSubversion -Control de versiones Java SvrSybase – BD. Sybase SvrMail01 – Servidor de correo XP-dad - Card al día SvrRcc – MS SQL Svrwebdesold - Desarrollo IIS SvrMysql – Mysql Producción WebDesLinux - Linux Desarrollo XP-TravelPta – Pta Travel Svrwebdes - Desarrollo	Falla de energía y otras interrupciones eléctricas		2	5	**20**	RT	* Independizar UPS para protección exclusiva de los equipos de C. Cómputo.	Reducir	2	C	1	5	**15**	TT	JCC
	Virus, troyanos, gusanos especializados que afecten específicamente servidores		3	5	**25**	RT	* Implementar informes mensuales sobre estado del antivirus * Habilitar archivo físico para informes mensuales visados. (J. CC)	Reducir	1	C	2	5	**20**	RT	JCC
	Mala manipulación de equipos		3	4	**22**	RT	* Capacitación a operadores * Actualización del MOF (detallando responsabilidades) * Elaborar instructivos técnicos sobre la función de los servidores * Asignar personal capacitado para el centro de Cómputo de contingencia	Transferir	2	C	1	4	**14**	TT	JCC
	Falla en Firewall		2	5	**20**	RT	* Implementar HA en firewall	Reducir	2	C	1	5	**15**	TT	JCC
	Equipo descontinuado		2	3	**16**	RT	* Establecer un inventario actualizado de equipos (vida útil) * Elaborar plan de renovación de equipos	Reducir	1	C	1	3	**13**	TT	JCC
	Saturación de Rack de servidores		1	5	**15**	TT	* Implementar nuevo Rack	Reducir	1	C	1	4	**14**	TT	JCC
	Sobrecarga de tráfico en red LAN		2	5	**20**	RT	* Implementar herramientas de monitoreo de tráfico	Reducir	2	C	1	5	**15**	TT	JCC
	Mala configuración		2	4	**18**	RT	* Implementar procedimientos de cambios de configuración	Reducir	1	C	1	4	**14**	TT	JCC

	IIS	Acceso no autorizado		2	5	**20**	RT	* Implementar control de claves a los servidores * Implementar control dual de clave maestra * Renovar el sistema de control de accesos de producción. * Cambiar la puerta de Data Center por una puerta de metal. * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia) * Implementar procedimientos de cambios de configuración	Reducir	3	M	1	5	**15**	TT	JCC
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)		3	4	**22**	RT	* Implementar programa de mantenimiento preventivo de equipos. * Implementar detectores para el control de temperatura * Implementar aire acondicionado de precisión * Implementar deshumedesedor	Reducir	2	C	1	4	**14**	TT	JCC

		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)		1	5	**15**	**TT**	* Implementar extintores de Gas Halotron y Polvo Químico seco * Capacitación en uso de extintores * Implementar detectores de aniego * Implementar contingencia de servidores. * Implementar aire acondicionado de precisión * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia)	Reducir	2	C	1	4	**14**	**TT**	JCC
		Robo de equipo		2	5	**20**	**RT**	* Implementar mecanismos para controlar el acceso físico al Centro de Cómputo. * Implementar controles físicos de seguridad	Reducir	2	C	1	5	**15**	**TT**	JCC
3	**Host Security Module:** HSM THALES PRODUCCION HSM THALES DESARROLLO HSM ATALLA PRODUCCION HSM ATALLA DESARROLLO	Falla de hardware	7	3	5	**22**	**RT**	* Implementar HSM ATALLA	Reducir	2	C	1	5	**12**	**TT**	JCC
		Desconfiguración de equipo		1	5	**12**	**TT**	* Actualización de manuales de configuración	Reducir	1	C	1	4	**11**	**TT**	JCC
		Pérdida de llaves maestras		2	5	**17**	**RT**	* Implementar mecanismos de control para las llaves maestras. (procedimientos, instructivos, formatos)	Reducir	1	C	1	5	**12**	**TT**	JCC
		Mala manipulación de equipos		3	4	**19**	**RT**	* Elaborar instructivos, políticas y procedimientos de operación y mantenimiento	Reducir	1	C	2	4	**15**	**TT**	JCC
		Falla de energía y otras interrupciones eléctricas		2	5	**17**	**RT**	* Independizar UPS para protección exclusiva de los equipos de C. Cómputo.	Reducir	2	C	1	5	**12**	**TT**	JCC

		Acceso no autorizado		2	5	**17**	**RT**	* Implementar control de claves a los servidores * Implementar control dual de clave maestra * Renovar el sistema de control de accesos de producción. * Cambiar la puerta de Data Center por una puerta de metal. * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia) * Implementar procedimientos de cambios de configuración	Reducir	3	M	1	5	**12**	**TT**	JCC
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)		2	4	**15**	**TT**	* Implementar extintores de Gas Halotron y Polvo Químico seco * Capacitación en uso de extintores * Implementar detectores de aniego * Implementar contingencia de servidores. * Implementar aire acondicionado de precisión * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia) * Implementar contingencia de HSM ATALLA	Reducir	3	M	1	4	**11**	**TT**	JCC
		Robo de equipo		2	5	**17**	**RT**	* Implementar mecanismos para controlar el acceso físico al Centro de Cómputo. * Implementar controles físicos de seguridad	Reducir	2	C	1	5	**12**	**TT**	JCC

4	**Central Telefónica:** Nortel Avaya	Falla de energía y otras interrupciones eléctricas	9	1	5	**14**	TT	* Reubicar el servidor AVAYA * Elaborara plan de mantenimiento preventivo. * Incluir los en el "proyecto de implementación UPS" para la oficina principal la conexión de la central nortel.	Reducir	2	C	1	5	**14**	TT	JCC
		Falla de hardware		2	5	**19**	RT	* Implementar contingencia de central AVAYA (***) * Migrar Equipo Nortel a otra central telefónica	Reducir	2	C	1	5	**14**	TT	JCC
		Falla en Firewall		1	5	**14**	TT	* Implementar HA en firewall	Reducir	2	C	1	3	**12**	TT	JCC
		Mala manipulación de equipos		3	4	**21**	RT	* Elaborar instructivos, políticas y procedimientos de operación y mantenimiento	Reducir	1	C	1	4	**13**	TT	JCC
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)		1	5	**14**	TT	* Traslado de central telefónica al Centro de Cómputo.	Reducir	2	C	1	3	**12**	TT	JCC
		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)		1	5	**14**	TT	* Traslado de central telefónica al Centro de Cómputo.	Reducir	2	C	1	3	**12**	TT	JCC
		Robo de equipo		2	5	**19**	RT	* Traslado de central telefónica al Centro de Cómputo.	Reducir	2	C	1	5	**14**	TT	JCC

5	Impresoras	Falla de hardware	5	2	3	**11**	TT	* Implementar programa de mantenimiento preventivo	Reducir	1	C	1	3	**8**	TT	JCC
		Mala manipulación de equipos		4	3	**17**	RT	* Capacitación en uso de equipos y seguridad a usuarios CP.	Reducir	1	C	1	3	**8**	TT	JCC
		fallas eléctricas		2	2	**9**	TT	---				2	2	**9**	TT	
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)		2	2	**9**	TT	* Implementar programa de mantenimiento preventivo	Reducir	1	C	1	2	**7**	TT	JCC
6	Teléfono	Robo de equipo	8	3	3	**17**	RT	* Implementar documentos para el retiro de equipos fuera de las instalaciones (políticas, formatos, procedimientos) * Implementar controles para visitas externas * Contar con un stock de contingencia	Reducir	1	C	1	3	**11**	TT	JCC
7	Firewall JUNIPER	Falla de hardware	7	1	5	**12**	TT	* Implementar informes mensuales sobre estado del antivirus * Habilitar archivo físico para informes mensuales visados. (J. CC)	Reducir	1	C	1	4	**11**	TT	JCC
		Mala manipulación de equipos		2	5	**17**	RT	* Planificar los trabajos de mantenimiento. * Elaborar instructivos técnicos de configuración.	Reducir	1	C	1	5	**12**	TT	JCC

		Acceso no autorizado		1	5	**12**	**TT**	* Implementar procedimiento de control de claves a los Firewall * Implementar procedimientos de cambios de configuración * Implementar control dual de clave maestra * Renovar el sistema de control de accesos de producción. * Cambiar la puerta de Data Center por * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia)	Reducir	2	C	1	4	**11**	**TT**	JCC
		Ataques externos		1	5	**12**	**TT**	* Implementar IPS	Reducir	3	C	1	4	**11**	**TT**	JCC
8	**Equipos de Comunicaciones:** Routers Switch Patch Panel	Robo de equipo	10	1	5	**15**	**TT**	* Contar con un stock mínimo de repuestos	Reducir	1	C	1	4	**14**	**TT**	JCC
		Equipo descontinuado		3	4	**22**	**RT**	* Renovación tecnológica (Switch)	Reducir	2	C	2	4	**18**	**RT**	JCC
		Falla de energía		2	4	**18**	**RT**	* Incluir los equipos en el "proyecto de implementación UPS" para la oficina principal.	Reducir	1	C	1	4	**14**	**TT**	JCC
		Robo de equipo		3	4	**22**	**RT**	* Implementar gabinetes con seguridad (todas las sedes)	Reducir	2	C	2	4	**18**	**RT**	JCC

		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)		2	4	**18**	**RT**	* Elaborar plan de mantenimiento preventivo	Reducir	1	C	1	4	**14**	**TT**	JCC
9	Blackberry	Robo de dispositivo	9	3	2	**15**	**TT**	---				3	2	**15**	**TT**	
		Mala manipulación de equipos		1	3	**12**	**TT**	---				1	3	**12**	**TT**	
		Acceso no autorizado		3	2	**15**	**TT**	* Configurar claves para equipos	Reducir	1	C	2	2	**13**	**TT**	JCC
		Pérdida de información		3	3	**18**	**RT**	* Capacitación a los usuarios en la seguridad de información * Elaborar procedimiento ante la pérdida de equipos	Reducir	1	C	2	3	**15**	**TT**	JCC
10	DSC 300 Storage	Mala manipulación de equipos	9	1	4	**13**	**TT**	----				1	4	**13**	**TT**	
		Acceso no autorizado		2	5	**19**	**RT**	* Renovar el sistema de control de accesos de producción. * Cambiar la puerta de Data Center por una puerta de metal. * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y	Reducir	2	C	1	5	**14**	**TT**	JCC

								Contingencia)										
		Falla de energía y otras interrupciones eléctricas		2	5	**19**	**RT**	* Independizar UPS para protección exclusiva de los equipos de C. Cómputo.	Reducir	2	C	1	5	**14**	**TT**	JCC
		Falla de hardware		1	5	**14**	**TT**	* Implementar HA de Storage * Implementar programa de mantenimiento preventivo de equipos. * Implementar mecanismos de control a los contratos de mantenimiento con terceros. * Seguimiento a las garantías * Mantener relaciones comerciales con proveedores estratégicos.	Reducir	2	C	1	4	**13**	**TT**	JCC
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)		3	4	**21**	**RT**	* Implementar programa de mantenimiento preventivo de equipos. * Implementar detectores para el control de temperatura * Implementar aire acondicionado de precisión * Implementar deshumedesedor	Reducir	2	C	2	4	**17**	**RT**	JCC

		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)		1	5	**14**	**TT**	* Implementar extintores de Gas Halotron y Polvo Químico seco * Capacitación en uso de extintores * Implementar detectores de aniego * Implementar contingencia de servidores. * Implementar aire acondicionado de precisión * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia)	Reducir	2	M	1	4	**13**	**TT**	JCC
11	**Unidades de Almacenamiento:** Unidades de cinta LTO4 Unidades de cinta LTO3 DLO Back UP	Acceso no autorizado	6	2	5	**16**	**RT**	* Renovar el sistema de control de accesos de producción. * Cambiar la puerta de Data Center por una puerta de metal. * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia)	Reducir	3	M	1	5	**11**	**TT**	JCC
		Falla de hardware		1	5	**11**	**TT**	* Implementar programa de mantenimiento preventivo de equipos. * Implementar mecanismos de control a los contratos de mantenimiento con terceros. * Seguimiento a las garantías * Mantener relaciones comerciales con proveedores estratégicos.	Reducir	1	C	1	4	**10**	**TT**	JCC
		Desconfiguracion de equipo		1	5	**11**	**TT**	* Actualización de manuales de configuración	Reducir	1	C	1	4	**10**	**TT**	JCC

		Falla de energía y otras interrupciones eléctricas		2	5	**16**	**RT**	* Independizar UPS para protección exclusiva de los equipos de C. Cómputo.	Reducir	2	C	1	5	**11**	**TT**	JCC
		Robo de equipos		3	3	**15**	**TT**	* Implementar mecanismos para controlar el acceso físico al Centro de Cómputo. * Implementar controles físicos de seguridad	Reducir	2	C	1	3	**9**	**TT**	JCC
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)		2	4	**14**	**TT**	* Elaborar plan de mantenimiento preventivo	Reducir	1	C	1	4	**10**	**TT**	JCC
12	UPS	Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)	10	3	4	**22**	**RT**	* Implementar programa de mantenimiento preventivo de equipos. * Implementar mecanismos de control a los contratos de mantenimiento con terceros. * Seguimiento a las garantías * Mantener relaciones comerciales con proveedores estratégicos.	Reducir	1	C	2	4	**18**	**RT**	JCC
		Fallas de equipos		1	5	**15**	**TT**	* Implementar HA de UPS * Implementar alertas automáticas * Implementar procedimientos y/o instructivos ante la falla de equipos	Reducir	2	C	1	4	**14**	**TT**	
		Equipo descontinuado		2	3	**16**	**RT**	* Establecer un inventario actualizado de equipos (vida útil) * Elaborar plan de renovación de equipos	Reducir	1	C	1	3	**13**	**TT**	JCC

		Desastres (fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural y hechas por el hombre)		1	5	**15**	TT	* Implementar extintores de Gas Halotron y Polvo Químico seco * Capacitación en uso de extintores * Implementar detectores de aniego * Implementar contingencia de servidores. * Implementar aire acondicionado de precisión * Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia)	Reducir	3	M	1	4	**14**	TT	JCC
13	Unidad de cinta	Robo de unidades de cinta	7	3	3	**16**	RT	* Implementar controles para visitas externas * Implementar controles para prevenir el acceso físico del personal a lugares restringidos. * Implementar mecanismos de encriptación	Reducir	1	C	1	3	**10**	TT	JCC
		Pérdida de información		2	3	**13**	TT	* Implementar pruebas periódicas de restauración.	Reducir	1	C	1	3	**10**	TT	JCC
		Deterioro de equipos debido a contaminación (Vibraciones, polvo, suciedad, humedad, insolación)		1	5	**12**	TT	* Implementar ubicaciones adecuadas para las cintas		1	C	1	4	**11**	TT	JCC

14	**Otros equipos:** Disco duro externo Triturador de papel Modem Claro S. Control de Acceso Periféricos	Robo de dispositivo	5	2	2	**9**	TT	* Implementar controles para visitas externas * Implementar controles para prevenir el acceso físico del personal a lugares restringidos.	Reducir	1	C	1	2	**7**	TT	JCC
		Pérdida de información		5	3	**20**	RT	* Implementar políticas y procedimientos para el uso de medios removibles	Reducir	1	C	2	3	**11**	TT	JCC
		Infección por código malicioso, virus, troyanos, gusanos		5	2	**15**	TT	* Implementar bitácora de control diario del estado del antivirus	Reducir	1	C	3	2	**11**	TT	JCC
15	**Base de Datos:** DB2 ORACLE MYSQL SYBASE	Mala manipulación de las Bases de Datos	10	5	5	**35**	NT	* Definir rol de DBA	Reducir	1	C	3	5	**25**	RT	JCC
		Fallas del software		2	5	**20**	RT	* Implementar plan de actualización de versiones * Implementar un plan de actualización de parches anual	Reducir	1	C	1	5	**15**	TT	JCC

		Acceso no autorizado a las BD		2	5	**20**	**RT**	* Definir roles para acceso a las BD y lineamientos para los cambios. * Implementar revisiones periódicas de accesos a BD. * Implementar solución de control de acceso y monitoreo de BD	Reducir	2	C	1	5	**15**	**TT**	JCC
		Modificación/Eliminación del la información por acceso no autorizado		5	5	**35**	**NT**	* Implementar solución de control de acceso y monitoreo de BD * Implementar control de claves a las BD * Implementar control dual de clave maestra	Reducir	2	C	3	5	**25**	**RT**	JCC
		Performance de la BD		3	5	**25**	**RT**	* Implementar de monitoreo de performance * Implementar procedimiento de afinamiento de BD (Reorganización de archivos, depuración, mejora de la performance de los programas)	Reducir	1	C	2	5	**20**	**RT**	JCC
		Robo de información de las BD		3	3	**19**	**RT**	* Implementar soluciones de encriptación y enmascaramiento de BD * Implementar solución de control de acceso y monitoreo de BD * Implementar control de claves a los servidores * Implementar control dual de clave maestra	Reducir	1	C	1	3	**13**	**TT**	JCC
16	**Herramientas de Gestión:** • Aranda Service Desk • Netsupport • VMWARE Wesphere	Acceso no autorizado	7	3	5	**22**	**RT**	* Implementar control de claves a los servidores * Implementar control dual de clave maestra	Reducir	1	C	1	5	**12**	**TT**	JCC

	• Aranda Inventory • Subversion • Page Device Control • Vision • Servidor de Correo • Sharepoint • Avaya • Symantec Backup Exec • DVR • DLO (BK PC 's) • Drupal • Vcenter **Herramientas de Seguridad Perimetral:** • AntiSpam • Filtro Web • Antivirus Kaspersky **Herramientas de Alta disponibilidad** **Herramienta de Inteligencia de Negocios** • Business Object	Fallas del software		2	5	**17**	RT	* Implementar plan de actualización de versiones * Implementar un plan de actualización de parches anual	Reducir	1	C	1	5	**12**	TT	JCC
		Mala configuración		2	5	**17**	RT	* Implementar procedimientos de cambios de configuración	Reducir	1	C	1	5	**12**	TT	JCC
		Desconfiguracion de software		1	2	**9**	TT	* Implementar base de conocimientos en Aranda Help Desk	Reducir	1	C	1	1	**8**	TT	JCC
		Mala manipulación de las herramientas		5	5	**32**	NT	* Elaborar instrucciones técnicas de trabajo	Reducir	1	C	2	5	**17**	RT	JCC
17	**Sistemas Operativos:** S.O. Windows Server Estándar S.O. Linux Redhat S.O. Unix S.O. OS/2	Infección por Virus, troyanos, gusanos, otros	10	3	5	**25**	RT	* Implementar informes mensuales sobre estado del antivirus * Habilitar archivo físico para informes mensuales visados. (J. CC) * Implementar bitácora de control diario del estado del antivirus	Reducir	1	C	1	5	**15**	TT	JCC
		Mala configuración		2	4	**18**	RT	* Implementar procedimientos de cambios de configuración	Reducir	1	C	1	4	**14**	TT	JCC

		Fallas del software		2	5	**20**	**RT**	* Implementar plan de actualización de versiones * Implementar un plan de actualización de parches anual	Reducir	1	C	1	5	**15**	**TT**	JCC
		Acceso no autorizado		2	5	**20**	**RT**	* Implementar control de claves a los servidores * Implementar control dual de clave maestra	Reducir	1	C	1	5	**15**	**TT**	JCC
18	Sistema de Control de Acceso físico	Falla de hardware	8	2	4	**16**	**RT**	* Renovación tecnológica	Reducir	2	C	1	3	**11**	**TT**	JCC
19	**Aplicativos:** MOC MCR MAG SIAF Sistema de Control de Cambios SPEED CADWEB CPCobranzas (recaudadoras y cartas) Estado cuenta web (generación de pdf's) Bridge (aplicativo recepción y envío de lote a DCI) Emisión de EECC y Doc. Aut. (Generación TxT para Urbano) Infocor APP Control Lotes Internacional	Acceso no autorizado	11	3	5	**26**	**NT**	* Implementar política de equipo desatendido. * Habilitar el protector de pantalla automático	Reducir	1	C	1	5	**16**	**RT**	JCC
		Desinstalación de aplicativos		3	5	**26**	**NT**	* Habilitar restricciones en el dominio para prohibir desinstalación de programas. * Habilitar el protector de pantalla automático * Habilitar restricciones de eliminación de iconos de escritorio.	Reducir	1	C	1	5	**16**	**RT**	JCC
		Errores en el despliegue de la aplicación		2	4	**19**	**RT**	* Mejorar el proceso de pase a producción *Mejorar el sistema de pases a producción	Reducir	1	C	1	4	**15**	**TT**	JCC

	APP Generación de Lotes Internacional Sistema de seguridad visual APP para Activación de tarjetas Disposición de efectivo (Banco Financiero) Global Vision APP GNI	Errores en el tratamiento de la información		5	5	**36**	**NT**	* Implementar mejoras en la certificación de aplicativos	Reducir	1	C	2	5	**21**	**RT**	JCC
20	Bitácora de procesos diarios	Pérdida física de bitácora	8	1	2	**10**	**TT**	* Escaneo de bitácora y almacenamientos por un año	Reducir	1	C	1	1	**9**	**TT**	JCC
		Modificación/Eliminación del formato		3	2	**14**	**TT**	* Formalizar formato de bitácora * Cambiar formato a PDF (Con seguridad)	Reducir	1	C	1	2	**10**	**TT**	JCC
		Mala ejecución de los procesos		3	3	**17**	**RT**	* Implementar instrucciones técnicas de trabajo * Capacitación en uso de la bitácora de procesos	Reducir	1	C	1	3	**11**	**TT**	JCC
21	Licencia de Tecnología Contratos de Mantenimiento Contratos de Soporte	Pérdidas de los documentos de licencia físicas y ausencia de control de renovaciones.	9	3	4	**21**	**RT**	* Elaborar plan de actualización de inventario de licencias * Digitalizar licencias físicas * Implementar mecanismos de control para renovación de licencias.	Reducir	1	C	2	4	**17**	**RT**	JCC
		Pérdida de los contratos físicos y ausencia de control de renovaciones.		3	4	**21**	**RT**	* Elaborar inventario de contratos * Digitalizar contratos físicas * Implementar mecanismos de control para renovación de contratos	Reducir	1	C	2	4	**17**	**RT**	JCC
		Mala interpretación de licencias		1	4	**13**	**TT**	---				1	3	**12**	**TT**	
		Mal uso de licencias		1	4	**13**	**TT**	* Implementar lineamientos para el uso de licencias.	Reducir	1	C	1	3	**12**	**TT**	JCC

22	**Servicios en Línea** Procesos MC (POS) Global NET (ATM) Pulse (ATM) DCISC (POS) Banco Financiero (D. Efectivo) Web Service movistar (DAD) Web Service Travel Account Bancared Internet CLARO Reniec Hermes Central de Riesgos	Falla en Firewall	7	1	5	**12**	TT	* Implementar HA en firewall	Reducir	2	C	1	4	**11**	TT	JCC
		Caída de servicio de internet		1	5	**12**	TT	* Implementar contingencia de internet	Reducir	2	C	1	4	**11**	TT	JCC
		Ataque externo		2	5	**17**	RT	* Implementar un IPS	Reducir	2	C	1	5	**12**	TT	JCC
		Indisponibilidad de los servicios		2	5	**17**	RT	* Elaborar lista de contactos * Elaborar procedimientos de comunicaciones	Reducir	1	C	1	5	**12**	TT	JCC
		Sobrecarga de tráfico en red LAN		2	2	**11**	TT	* Implementar monitoreo de red	Reducir	1	C	1	2	**9**	TT	JCC
23	**Servicios en Lotes** Procesos MC Global Net DCISC (Xchange, Settlement) Banco Financiero IATA Recaudación Bancos CAD TACA Coris Courier (Urbano) Web Service PNR - Empresas Verificadoras Venta de Cartera de Bancos Central de Riesgos	Mala ejecución de los procesos	6	3	4	**18**	RT	* Implementar instrucciones técnicas de trabajo * Capacitación en uso de la bitácora de procesos * Implementar mecanismos de control y seguimiento	Reducir	1	C	1	4	**10**	TT	JCC
		Archivos recibidos erróneos		2	3	**12**	TT	* Implementar mecanismos de consistencia de la información	Reducir	1	C	1	3	**9**	TT	JCC
		Indisponibilidad de los servicios		2	3	**12**	TT	* Elaborar lista de contactos * Elaborar procedimientos de comunicaciones	Reducir	1	C	1	3	**9**	TT	JCC
		Manipulación de la información		2	3	**12**	TT	* Implementar medios de transmisión seguros	Reducir	1	C	1	3	**9**	TT	JCC
		Caída de servicio de internet		2	3	**12**	TT	* Implementar contingencia de internet	Reducir	2	C	1	3	**9**	TT	JCC
		Falla en Firewall		2	5	**16**	RT	* Implementar HA en firewall	Reducir	2	C	1	4	**10**	TT	JCC

24	**Servicios FTP (terceros) :** Banco Financiero Urbano Procesos MC Data Crédito Ocasa SMP Pulse Supermercados Peruanos	Falla en Firewall	6	1	5	**11**	TT	* Implementar HA en firewall	Reducir	2	C	1	4	**10**	TT	JCC
		Sobrecarga de tráfico en red LAN		2	2	**10**	TT	* Implementar monitoreo de red	Reducir	1	C	1	2	**8**	TT	JCC
		Perdida de usuario/clave		2	5	**16**	RT	* Elaborar inventario de servicios FTP (información sobre uso, datos de acceso) * Implementar control de claves	Reducir	1	C	1	5	**11**	TT	JCC
25	Jefe Centro Cómputo Jefe de Producción Coordinar de Networking Analista de Help Desk Asistentes de Help Desk Administrador de Red Operadores de Producción	Indisponibilidad del personal	7	3	3	**16**	RT	* Establecer y difundir procedimientos y políticas * Elaborar y difundir MOFs * Mantener actualizado la información la documentación.	Reducir	1	C	1	3	**10**	TT	JCC
		Carencia de conocimiento en tecnologías o herramientas implementadas		2	3	**13**	TT	* Elaborar plan de capacitación anual (nuevas tecnologías)	Reducir	1	C	1	3	**10**	TT	JCC
		Ausencia de cultura en seguridad de la información		2	3	**13**	TT	* Implementa programa de capacitación y sensibilización al personal en seguridad de información	Reducir	1	C	1	3	**10**	TT	JCC
		Robo de información		3	2	**13**	TT	* Implementar compromiso de confidencialidad de información	Reducir	1	C	2	2	**11**	TT	JCC
		Extorsión		1	3	**10**	TT	---				1	3	**10**	TT	

Cuadro 3.24: Gestión de riesgos de departamento de centro de cómputo [58]

[58] Elaboración: los autores.

3.2.2.5 Plan de tratamiento del riesgo

A) Plan de tratamiento de riesgos – Desarrollo

PLAN TRABAJO PARA EL TRATAMIENTO DE RIESGOS - DESARROLLO								
Nro.	**MECANISMOS DE PROTECCIÓN**	**ACTIVIDADES**		**Plazo**		**Avance %**	**Responsables**	**Tiempo Estimado**
				Inicio	**Fin**			
1	* Actualizar los estándares de programación	**1.1**	* Revisión de los estándares de programación para aplicativos AS/400	02/02/2012	02/02/2012	100%	Analista Programador	6hs
		1.2	* Redefinición de estándares de programación para aplicativos AS/400	03/02/2012	03/02/2012	100%	Analista Programador- Jefe Desarrollo	6hs
		1.3	* Publicación de los estándares de programación para aplicativos AS/400	03/02/2012	03/02/2012	100%	Jefe Desarrollo	1hs
		1.4	* Inducción/Difusión al personal de desarrollo, sobre los estándares programación para aplicativos AS/400	06/02/2012	06/02/2012	100%	Jf. Proyectos	1hs
2	* Auditoría de código fuente (Visual, NET, Java, AS/400)	**2.1**	* Contrato de especialista en auditoria de códigos fuente	06/02/2012	14/02/2012	100%	GLEGAL - GTI	7ds
		2.2	* Elaboración del Plan de auditoria anual	15/02/2012	07/03/2012	100%	Jefe Desarrollo	16hs
		2.3	* Ejecución de la primera auditoría	08/03/2012	09/03/2012	100%	Especialista Auditor	1ds
		2.4	* Ejecución de las Acciones Correctivas / Preventivas	12/03/2012	23/03/2012	100%	Jefe Desarrollo - Jf. Proyectos - EQUIPO DESARROLLO	10ds
3	* Concientizar al personal sobre la Seguridad de Información	**3.1**	* Elaborar plan de concientización en seguridad de información	03/02/2012	06/02/2012	100%	Jefe Desarrollo	8hs
		3.2	* Elaborar material de concientización / difusión	06/02/2012	07/02/2012	100%	Jefe Desarrollo	8hs

		3.3	* Ejecutar primera concientización en Seguridad de Información	07/02/2012	08/02/2012	100%	Jefe Desarrollo	2hs
4	* Configurar accesos a carpetas por perfiles a la documentación * Implementar controles para protección de documentos	**4.1**	* Definir alternativas de estructura de almacenamiento (SharePoint / carpetas)	09/02/2012	10/02/2012	100%	Jefe Desarrollo - Jf. Proyectos	16hs
		4.2	* Ejecución de alternativa seleccionada	06/02/2012	07/02/2012	100%	Jf. Producción	8hs
		4.3	* Configuración de permisos por roles	07/02/2012	07/02/2012	100%	Jf. Producción	3hs
5	* Configurar accesos por perfiles a la Base de Datos (MySQL)	**5.1**	Elaborar inventario de usuarios vs Base de Datos	08/02/2012	08/02/2012	100%	Jf. Producción - Jefe Desarrollo	3hs
		5.2	Asignar accesos a usuarios	08/02/2012	08/02/2012	100%	Jf. Producción	2hs
6	* Contrato de confidencialidad con los proveedores	**6.1**	* Definición con área legal tipos de documentos para establecer confidencialidad con proveedores	13/02/2012	21/02/2012	100%	Gerencia Tecnología Gerente Tecnología / Legal	7ds
		6.2	* Elaboración de Documentos definidos	21/02/2012	23/02/2012	100%	Jefe Desarrollo	16hs
		6.3	* Aprobación de documentos	23/02/2012	23/02/2012	100%	Jefe Desarrollo - Gerente Tecnología	2hs
7	* Encriptación/Enmascaramiento de la información de las bases de datos	**7.1**	* Definir herramienta de encriptación	23/02/2012	24/02/2012	100%	Jefe Desarrollo - Jf. Producción	16hs
		7.2	* Evaluar/Desarrollar herramienta	25/02/2012	25/02/2012	100%	Jefe Desarrollo	2hs
		7.3	* Implementar herramienta	25/02/2012	25/02/2012	100%	Jf. Producción	4hs
8	* Personalizar entrega de fuentes a proveedores	**8.1**	* Definir ambientes de trabajo para proveedores en las diferentes plataformas (AS/400, Visual, .NET, Java)	25/02/2012	26/02/2012	100%	Jf. Proyectos - Analista Programador	4hs

		8.2	* Implementar ambiente de trabajo restringido para plataforma AS/400	26/02/2012	26/02/2012	100%	Jf. Proyectos - Jf. Producción	4hs
		8.3	* Implementar ambientes de trabajo restringido para plataforma JAVA	26/02/2012	27/02/2012	100%	Jf. Proyectos - Jf. Producción	4hs
		8.4	* Implementar ambientes de trabajo restringido para plataforma Visual Basic y .NET	27/02/2012	27/02/2012	100%	Jf. Proyectos - Jf. Producción	4hs
9	* Definir canales de comunicación eficiente con proveedores de servicios en línea y en lotes	**9.1**	* Definir el canal formal de comunicación entre Card Perú y (Procesos MC, Global Net, DCISC (Exchange, Settlement), Banco Financiero), para reportar incidencias en producción.	28/02/2012	28/02/2012	100%	Jefe Desarrollo - Jf. Proyectos	4hs
10	* Implementar verificación de los campos de las tramas de autorizaciones para los servicios en línea y en lotes.	**10.1**	* Definir con Gerencia Operaciones controles a implementar por cada servicio	01/03/2012	21/03/2012	100%	Jf. De Desarrollo	15ds
		10.2	* Definir con Gerencia de Operaciones protocolos a seguir por cada servicio	21/03/2012	27/03/2012	100%	Jf. De Desarrollo	5ds
		10.3	* Ejecutar controles aprobados	27/03/2012	09/04/2012	100%	Jf. De Desarrollo	10ds
		10.4	* Difundir a Centro de Cómputo los controles implementados y protocolos a seguir	09/04/2012	10/04/2012	100%	Jf. De Desarrollo	2ds
12	* Desarrollar sistema de control de accesos por aplicativo. * Mejorar el proceso de reserva de fuentes.	**12.1**	* Evacuación y adquisición de software especializado para el control de accesos	20/02/2012	21/02/2012	100%	Jf. Proyectos	16hs
13	* Documentar los procesos del planificador	**13.1**	* Documentar los procesos del planificador para los procesos en lotes	06/02/2012	10/02/2012	100%	Analista Programador - Jf. Producción	5ds
		13.2	* Capacitación al personal de desarrollo en procesos del planificador	13/02/2012	13/02/2012	100%	Analista Programador	2hs

14	* Analizar procesos bacheros previo al pase a producción.	**14.1**	* Elaborar lineamientos para analizar procesos bacheros previo al pase a producción.	11/04/2012	11/04/2012	100%	Jefe Desarrollo	4hs
14.5	* Depuración de procesos bacheros no vigentes	**14.5.1**	* Elaborar lineamientos la depuración de procesos bacheros no vigentes	14/02/2012	14/02/2012	100%	Analista Programador - Jf. Producción - Jf. Proyectos	8hs
		14.5.2	* Depuración de procesos bacheros no vigentes.	15/02/2012	15/02/2012	100%	Jf. Producción	2hs
15	* Elaborar contratos modelos para la tercerización de desarrollos / Elaborar cláusula de penalidades por incumplimiento de plazos.	**15.1**	* Definición con área legal modelos de contratos para tercerización de desarrollos con proveedores	27/02/2012	29/02/2012	100%	Gerencia Tecnología Gerente Tecnología / Legal	3ds
		15.2	* Aprobación de documentos	29/02/2012	01/03/2012	100%	Gerencia Tecnología Gerente Tecnología / Legal	1ds
16	* Elaborar documentación técnica de los desarrollos	**16.1**	* Elaborar matriz para control de entrega de documentos de los proyectos (2012 en adelante)	05/03/2012	05/03/2012	100%	Jf. Proyectos - Jefe Desarrollo	3hs
17	* Dimensionar licencias según las demandas presentes y futuras. * Administración de Licencias * Implementar controles y revisiones anuales para las renovaciones de licencias.	**17.1**	* Elaborar lineamientos para la gestión de licencias	05/03/2012	05/03/2012	100%	Jefe Desarrollo	4hs
		17.2	* Ejecutar primera revisión del inventario de licencias	06/03/2012	07/03/2012	100%	Jefe Desarrollo - Jf. Proyectos	2hs
18	* Entrenamiento de personal en protocolo de comunicaciones	**18.1**	* Entrenamiento de personal en protocolo de comunicaciones ISO 8583	07/03/2012	07/03/2012	100%	Jefe Desarrollo	2hs
19	* Establecer una línea segura para el intercambio de información.	**19.1**	* Identificar información que se intercambia por correo electrónico.	07/03/2012	07/03/2012	100%	Analista Programador	4hs

	(servicios bacheros y en línea)						- Jf. Producción	
		19.2	* Migrar intercambio de información a línea segura (FTP)	08/03/2012	08/03/2012	100%	Jf. Producción	4hs
		19.3	* Establecer lineamientos de línea segura	09/03/2012	09/03/2012	100%	Jefe Desarrollo- Jefe de Producción	4hs
20	* Elaborar y difundir MOFs * Mantener actualizado la información la documentación.	**20.1**	* Elaborar/Actualizar MOF de personal de desarrollo	10/03/2012	10/03/2012	100%	Jefe Desarrollo	2hs
		20.2	* Difundir MOF a todo el personal de desarrollo	10/03/2012	10/03/2012	100%	Jefe Desarrollo	1hs
21	* Estandarizar y difundir métodos de ejecución de pruebas unitarias	**21.1**	* Capacitar a los desarrolladores en técnicas para la elaboración de pruebas unitarias	13/02/2012	17/02/2012	100%	Analista Calidad	5ds
22	* Formalizar la metodología de Atención de RQ * Capacitar / Concientizar a los usuarios	**22.1**	* Elaborar procedimientos y formatos para la metodología de Atención de Requerimientos	11/03/2012	11/03/2012	100%	Jefe Desarrollo	8hs
		22.2	* Aprobar procedimientos y formatos	12/03/2012	12/03/2012	100%	Jefe Desarrollo - Gerente Tecnología	2hs
		22.3	* Difusión y Capacitación a personal de desarrollo y usuarios finales	12/03/2012	12/03/2012	100%	Jefe Desarrollo	2hs
23	* Formalizar la metodología de Ingeniería de Software * Capacitar / Concientizar a los usuarios	**23.1**	* Elaborar procedimientos y formatos para la metodología de Ingeniería de Software	13/03/2012	13/03/2012	100%	Jefe Desarrollo	8hs
		23.2	* Aprobar procedimientos y formatos	14/03/2012	14/03/2012	100%	Jefe Desarrollo - Gerente Tecnología	2hs
		23.3	* Difusión y Capacitación a personal de desarrollo y usuarios finales	14/03/2012	14/03/2012	100%	Jefe Desarrollo	2hs

24	* Implementar compromiso de confidencialidad * Implementar una política de confidencialidad	**24.1**	*Definición con área legal tipos de documentos para establecer confidencialidad de personal interno	02/03/2012	02/03/2012	100%	Gerente Tecnología - GLEGAL	4hs
		24.2	* Aprobación de documentos	05/03/2012	05/03/2012	100%	Gerente Tecnología - GLEGAL	4hs
25	* Implementar instructivos de instalación	**25.1**	* Elaborar instructivos de instalación para el AS/400	12/03/2012	12/03/2012	100%	Analista Programador - Analista Help Desk	2hs
		25.2	* Elaborar instructivos de instalación para el Visual	12/03/2012	13/03/2012	100%	Analista Programador - Analista Help Desk	8hs
		25.3	* Elaborar instructivos de instalación para el .Net	13/03/2012	14/03/2012	100%	Analista Programador - Analista Help Desk	8hs
26	* Implementar manuales, videos, tutoriales para los software	**26.1**	* Identificar necesidad de manuales, videos, tutoriales para los software utilizados	14/03/2012	14/03/2012	100%	Analista Programador - Analista Help Desk	4hs
		26.2	* Implementar manuales, videos, tutoriales para los software	15/03/2012	15/03/2012	100%	Analista Programador - Analista Help Desk	8hs
27	* Migración de aplicativos críticos de MySQL a Otra BD.	**29.1**	* Identificar aplicativos que interactúan con BD MySQL	06/03/2012	06/03/2012	100%	Jf. Proyectos - Analista Programador	8hs
		29.2	* Planificar migración de aplicativos MySQL	07/03/2012	07/03/2012	100%	Jf. Proyectos - Analista Programador	8hs
		29.3	* Ejecutar migración	19/03/2012	23/03/2012	100%	Analista Programador -	5ds

							Desarrollador	
28	* Implementar procedimiento para el desarrollo de aplicativos con terceros	**30.1**	* Elaborar procedimientos para el desarrollo de aplicativos con terceros	12/04/2012	12/04/2012	100%	Jefe Desarrollo - PROCESOS	8hs
		30.2	* Revisar y aprobar procedimientos / formatos	05/03/2012	05/03/2012	100%	Gerente Tecnología - Jefe Desarrollo	2hs
29	* Implementar procedimientos e instructivos para configurar ambientes de prueba (Servicios bach y en línea)	**31.1**	* Elaborar procedimientos e instructivos para configuración de ambientes de prueba para los servicios en bach	13/04/2012	13/04/2012	100%	Jefe Desarrollo - Jf. Proyectos - PROCESOS	8hs
		31.2	* Revisar y aprobar procedimientos (bach)	05/03/2012	05/03/2012	100%	Gerente Tecnología - Jefe Desarrollo	2hs
		31.3	* Elaborar procedimientos e instructivos para configuración de ambientes de prueba para los servicios en línea	14/04/2012	14/04/2012	100%	Jefe Desarrollo - Jf. Proyectos - PROCESOS	8hs
		31.3	* Revisar y Aprobar procedimientos (online)	06/03/2012	06/03/2012	100%	Gerente Tecnología - Jefe Desarrollo	2hs
30	* Implementar un laboratorio para las pruebas de cambios de versiones	**32.1**	* Elaborar procedimientos / formatos para implementar laboratorio de pruebas	15/04/2012	15/04/2012	100%	Jefe Desarrollo - Jf. Proyectos - PROCESOS	8hs
		32.2	* Revisar y Aprobar procedimientos	06/03/2012	06/03/2012	100%	Gerente Tecnología - Jefe Desarrollo	2hs
31	* Implementar un sistema de control	**33.1**	* Definir herramienta para control de versiones	16/04/2012	19/04/2012	100%	Jefe Desarrollo	16hs

	de versiones * Planificación del cambio de versiones.	**33.2**	* Evaluar herramienta especializada	20/04/2012	20/04/2012	100%	Jefe Desarrollo - Jf. Proyectos	8hs
		33.3	* Implementar herramienta especializada	08/03/2012	13/03/2012	100%	Jf. Proyectos - Analista Help Desk	4ds
32	* Separar los ambientes de contingencia, calidad y desarrollo.	**34.1**	Separar los ambientes de contingencia, calidad y desarrollo.	20/02/2012	11/05/2012	100%	Jf. Centro de Cómputo	60ds
33	* Mejorar el proceso de reserva y desarrollo de fuentes para aplicativos Java.	**35.1**	* Revisar estructura de los proyectos java	22/04/2012	22/04/2012	100%	Jefe Desarrollo - Arquitecto Sftw.	4hs
		35.2	* Ejecutar mejoras a los proyectos java	23/04/2012	25/04/2012	100%	Arquitecto Sftw. - Jf. Proyectos - Desarrollador	2ds
34	* Planificar la migración de aplicativos a java.	**36.1**	* Elaborar inventario de todos los aplicativos Visual Basic y. NET	22/04/2012	22/04/2012	100%	Jefe Desarrollo - Jf. Proyectos	4hs
		36.2	* Catalogar y priorizar aplicativos	22/04/2012	22/04/2012	100%	Jefe Desarrollo	1hs
		36.3	* Planificar migración de aplicativos VB y .NET	22/04/2012	23/04/2012	100%	Jefe Desarrollo - Jf. Proyectos	4hs
		36.4	* Ejecución de migraciones	11/02/2012	11/05/2012	100%	Jf. Proyectos - Desarrollador	90ds
35	* Reforzar el compromiso de las gerencias con la ejecución de las pruebas	**37.1**	* Reforzar el compromiso de las gerencias con la ejecución de las pruebas de los usuarios finales	23/04/2012	23/04/2012	100%	Jefe Desarrollo - Gerente Tecnología	2hs
36	* Revisiones periódicas de nuevas actualizaciones.	**38.1**	* Elaborar lineamientos de nuevas actualizaciones	26/04/2012	26/04/2012	100%	Jefe Desarrollo	6hs
		38.2	* Ejecutar primera revisión de nuevas versiones de los aplicativos	26/04/2012	27/04/2012	100%	Jefe Desarrollo	4hs

37	* Revisiones trimestrales de la documentación de proyectos del Jefe de Desarrollo.	**39.1**	¨Elaborar lineamientos para las revisiones de la documentación	27/04/2012	28/04/2012	100%	Jefe Desarrollo	6hs
		39.2	* Ejecutar primera revisión de cumplimiento de documentación de proyectos	28/04/2012	29/04/2012	100%	Jefe Desarrollo	4hs
38	*Actualizar el sistema de control de cambios para el pase a producción desde ambiente de certificación.	**42.1**	* Definir herramienta de control de cambios	30/04/2012	03/05/2012	100%	Jefe Desarrollo - Jf. Proyectos	2ds
		42.2	* Evaluar herramienta especializada	04/05/2012	04/05/2012	100%	Jefe Desarrollo - Jf. Proyectos - Analista Calidad	8hs
		42.3	* Implementar herramienta especializada	30/04/2012	04/05/2012	100%	Jf. Proyectos - Analista Help Desk	5ds

Cuadro 3.25: Plan de tratamiento de riesgos de departamento de centro de cómputo [59]

[59] Elaboración: los autores.

B) Plan de tratamiento de riesgos – Business intelligence

PLAN TRABAJO PARA EL TRATAMIENTO DE RIESGOS - BUSINESS INTELLIGENCE								
Nro.	**MECANISMOS DE PROTECCIÓN**	**ACTIVIDADES**		**Plazo**		**Avance %**	**Responsables**	**Tiempo Estimado**
				Inicio	**Fin**			
1	* Administración de Licencias * Elaborar un plan de dimensionamiento de licencias según las demandas presentes y futuras. * Implementar controles y revisiones mensuales para las renovaciones de licencias.	**1.1**	Elaborar lineamientos para la gestión de licencias	01/02/2012	01/02/2012	100%	Jf. Centro de Cómputo/Coordinador BI	2hrs
		1.2	Ejecutar primera revisión del inventario de licencias	01/02/2012	01/02/2012	100%	Jf. Centro de Cómputo/Coordinador BI	2hrs
		1.3	Definir criterios de dimensionamiento de licencias	02/02/2012	02/02/2012	100%	Coordinador BI/Analista BI	1hrs
		1.4	Realizar dimensionamiento anual de licencias.	03/02/2012	03/02/2012	100%	Coordinador BI	2hrs
2	* Alertas, seguimiento, reportes, etc. sobre el servicio de Base de Datos	**2.1**	Elaborar inventario de servicios críticos del servidor.	03/02/2012	03/02/2012	100%	Jf. Centro de Cómputo/Coordinador BI	2hrs
		2.2	Identificar alertas a configurar por cada servicio.	03/02/2012	03/02/2012	100%	Coordinador BI	1hrs
		2.3	Configurar alertas de problema en el servicio.	04/02/2012	04/02/2012	100%	Jf. Centro de Cómputo	1ds
		2.4	Definir reportes periódicos de performance del servidor.	03/02/2012	03/02/2012	100%	Coordinador BI	1hrs
		2.5	Configurar y programar reportes periódicos de la performance del servidor.	05/02/2012	05/02/2012	100%	Jf. Centro de Cómputo	1ds
		2.6	Configura reportes periódicos de seguimiento de espacio disponible en el disco duro.	06/02/2012	06/02/2012	100%	Jf. Centro de Cómputo	1ds
3	* Definir e Implementar control de versiones de programas BI.	**3.1**	Definir herramienta para control de versiones.	06/02/2012	17/02/2012	100%	Coordinador BI	10ds
		3.2	Evaluar herramienta especializada.	20/02/2012	26/03/2012	100%	Coordinador BI	30ds

		3.3	Implementar herramienta especializada.	27/03/2012	09/04/2012	100%	Coordinador BI	20ds
4	* Implementar pases a producción para programas SQL	**4.1**	Actualizar documento de pase a producción de programas BI.	09/04/2012	09/04/2012	100%	Coordinador BI	2hrs
		4.2	Revisar y validar documento con la Gerencia de Tecnología.	10/04/2012	10/04/2012	100%	Gerente/Coordinador BI	1hrs
		4.3	Formalizar y publicar documento.	10/04/2012	10/04/2012	100%	GDP	1hrs
		4.4	Capacitar a usuarios involucrados.	10/04/2012	10/04/2012	100%	Coordinador BI	1hrs
5	* Definir tiempos de Back UP	**5.1**	Definir tiempo de generación y permanencia de Back UP	10/04/2012	10/04/2012	100%	Coordinador BI	2hrs
6	* Definir y configurar el control de accesos por roles (documentos, base de datos)	**6.1**	Definir roles en base a responsabilidades.	11/04/2012	11/04/2012	100%	Coordinador BI	4hrs
		6.2	Definir accesos por rol.	11/04/2012	11/04/2012	100%	Coordinador BI	4hrs
		6.3	Asignar y configurar accesos	12/04/2012	12/04/2012	100%	Jf. Centro de Cómputo/Coordinador BI	2hrs
		6.4	Validar los accesos	12/04/2012	12/04/2012	100%	Jf. Centro de Cómputo/Coordinador BI	2hrs
7	* Definir y configurar el control de accesos por roles para la documentación de proyectos * Implementar inventario de documentos y control de cambios.	**7.1**	Definir alternativas de estructura de almacenamiento (SharePoint / carpetas)	01/02/2012	01/02/2012	100%	Coordinador BI/Analista BI	2hrs
		7.2	Ejecución de alternativa seleccionada	06/02/2012	06/02/2012	100%	Analista BI	4hrs
		7.3	Configuración de permisos por roles	01/02/2012	01/02/2012	100%	Coordinador BI	3hrs
		7.4	Configuración de control de cambios	06/02/2012	06/02/2012	100%	Analista BI	3hrs
8	* Definir y configurar el control de accesos por roles para las bases de datos	**8.1**	Elaborar inventario de usuarios que acceden actualmente a la BD.	12/04/2012	12/04/2012	100%	Coordinador BI	1hrs

	* Definir y configurar el control de accesos por roles para manipulación de bases externas * Implementar controles de acceso a las plataformas y los códigos fuente. * Implementar inventario de documentación del código fuente.	**8.2**	Identificar roles a configurar.	13/04/2012	13/04/2012	100%	Coordinador BI	2hrs
		8.3	Identificar accesos por rol.	13/04/2012	13/04/2012	100%	Coordinador BI	2hrs
		8.4	Configurar roles y accesos de base de datos.	16/04/2012	16/04/2012	100%	Jf. Centro de Cómputo/Coordinador BI	3hrs
		8.5	Asignar roles por usuario.	16/04/2012	16/04/2012	100%	Jf. Centro de Cómputo/Coordinador BI	2hrs
		8.6	Validar asignación de roles y accesos.	17/04/2012	17/04/2012	100%	Coordinador BI	2hrs
		8.7	Elaborar documento de roles y accesos.	07/02/2012	07/02/2012	100%	Analista BI	1ds
		8.8	Capacitar a Producción en la asignación de roles y actualización de documento.	08/02/2012	08/02/2012	100%	Analista BI	2hrs
9	* Desarrollar programas que remplacen las macros	**9.1**	Realizar inventario de macros implementadas.	08/02/2012	08/02/2012	100%	Analista BI	1hrs
		9.2	Explicar a detalle la funcionalidad a Desarrollo.	09/02/2012	09/02/2012	100%	Analista BI	4hrs
		9.3	Dar seguimiento a la implementación de programas.	12/04/2012	11/05/2012	100%	Coordinador BI/Analista BI	30ds
		9.4	Realizar pruebas.	12/05/2012	12/05/2012	100%	Coordinador BI/Analista BI	2ds
		9.5	Capacitar a usuarios involucrados.	28/03/2012	29/03/2012	100%	Analista BI	2ds
10	* Elaborar y difundir MOFs (incluir Seguridad de Información) * Establecer y difundir procedimientos y políticas * Mantener actualizado la información la documentación.	**10.1**	Revisar Análisis de Puestos elaborado.	21/02/2012	21/02/2012	100%	Gerente/Coordinador BI	4hrs
		10.2	Actualizar y validar Análisis de Puestos.	21/02/2012	21/02/2012	100%	Coordinador BI	2hrs
		10.3	Enviar a RRHH el Análisis de Puestos para su revisión, aceptación y publicación.	22/02/2012	24/02/2012	100%	Gerente/Coordinador BI	3ds
11	* Revisiones periódicas del Coordinador de B.I.	**11.1**	Elaborar Plan de revisiones de documentación.	27/02/2012	27/02/2012	100%	Coordinador BI	2hrs

12	* Implementar ambientes de desarrollo diferente al de producción. * Implementar ambientes de desarrollo.	**12.1**	Elaborar documento de especificaciones de servidor de desarrollo.	27/02/2012	27/02/2012	100%	Coordinador BI	2hrs
		12.2	Implementar servidor de desarrollo.	25/02/2012	26/03/2012	100%	Jf. Centro de Cómputo	30ds
		12.3	Configurar servidor.	27/02/2012	29/02/2012	100%	Jf. Centro de Cómputo/Coordinador BI	3ds
		12.4	Importar datos.	01/03/2012	01/03/2012	100%	Jf. Centro de Cómputo/Coordinador BI	5hrs
		12.5	Asignar accesos a usuarios.	01/03/2012	01/03/2012	100%	Jf. Centro de Cómputo/Coordinador BI	2hrs
		12.6	Validar implementación	02/03/2012	02/03/2012	100%	Coordinador BI	2hrs
13	* Revisiones periódicas de nuevas actualizaciones de software.	**13.1**	Elaborar plan de revisiones periódicas de actualización de software.	02/03/2012	02/03/2012	100%	Coordinador BI	2hrs
14	* Implementar controles de procesamientos de información	**14.1**	Elaborar inventario de procesos de carga al Datawarehouse.	02/03/2012	02/03/2012	100%	Coordinador BI/Desarrollador BI	1hrs
		14.2	Elaborar inventario de controles de procesos a implementar.	05/03/2012	05/03/2012	100%	Coordinador BI/Desarrollador BI	2hrs
		14.3	Implementar controles.	05/03/2012	09/03/2012	100%	Desarrollador BI	5ds
		14.4	Elaborar reportes periódicos de ejecución de procesos.	12/03/2012	14/03/2012	100%	Desarrollador BI	3ds
15	* Implementar controles de validación de información procesada	**15.1**	Elaborar inventario de tablas del Datawarehouse.	15/03/2012	16/03/2012	100%	Desarrollador BI	2ds
		15.2	Identificar métodos de validación por cada tabla procesada.	29/03/2012	04/04/2012	100%	Analista BI/Desarrollador BI	5ds
		15.3	Implementar reportes y controles de validación de información.	04/04/2012	24/04/2012	100%	Jf. Desarrollo / Desarrollador BI	15ds

16	* Implementar enmascaramiento/encriptación de datos.	**16.1**	Implementar herramienta especializada para el enmascaramiento y encriptación de datos	06/03/2012	06/04/2012	100%	Jf. Centro de Cómputo/Coordinador BI	30ds
17	* Implementar manuales, videos, tutoriales para los software	**17.1**	Elaborar inventario de software utilizado en BI.	07/04/2012	07/04/2012	100%	Coordinador BI	2hrs
		17.2	Elaborar manuales de instalación y configuración.	25/04/2012	25/04/2012	100%	Desarrollador BI	4hrs
		17.3	Capacitar.	25/04/2012	25/04/2012	100%	Desarrollador BI	2hrs

Cuadro 3.25: Plan de tratamiento de riesgos de departamento de business intelligence [60]

C) Plan de tratamiento de riesgos – Centro de cómputo

PLAN TRABAJO PARA EL TRATAMIENTO DE RIESGOS - CENTRO DE CÓMPUTO							
Nro.	**MECANISMOS DE PROTECCIÓN**	**ACTIVIDADES**		**Plazo**		**Avance %**	**Responsables**
				Inicio	**Fin**		
1	* Actualización de manuales de configuración	**1.1**	Elaborar manuales de configuración de HSM	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		1.2	Elaborar instructivos de configuración de respaldo y restauración para servidores INTEL	01/02/2012	16/02/2012	100%	Coordinador I&N
		1.3	Revisión y Aprobación de Manuales	20/02/2012	02/03/2012	100%	Jf. Centro Cómputo
2	* Implementa programa de capacitación y sensibilización al personal en seguridad de información	**2.1**	Elaborar presentación de capacitación en Seguridad de Información	06/02/2012	17/02/2012	100%	Oficial de Seg. Info.
		2.2	Elaborar boletines de Seguridad de Información	20/02/2012	09/03/2012	100%	Oficial de Seg. Info.

[60] Elaboración: los autores.

		2.3	Ejecutar Capacitación en Seguridad de Información	12/03/2012	23/03/2012	100%	Oficial de Seg. Info.
3	* Elaborar procedimiento ante la pérdida de equipos blackberry	**3.1**	Elaborar procedimiento ante la pérdida o robo de equipos blackberry	01/02/2012	01/02/2012	100%	Administrador de Red
		3.2	Revisión y Aprobación de procedimiento	20/02/2012	02/03/2012	100%	Jf. Centro Cómputo
4	* Capacitación al equipo de administración en cuidado de equipos	**4.1**	Elaborar un plan de capacitación en equipos de cómputo	02/02/2012	14/02/2012	100%	Analista Help Desk
		4.2	Capacitar al Equipo de mantenimiento en cuidado de equipos de cómputo (impresoras, laptop, PC's, otros)	14/02/2012	15/02/2012	100%	Analista Help Desk
5	* Capacitación en uso de equipos de cómputo	**5.1**	Elaborar un plan de capacitación en equipos de cómputo	16/02/2012	29/02/2012	100%	Analista Help Desk
		5.2	Capacitar a los usuarios en cuidado de equipos de cómputo (impresoras, laptop, PC's, otros)	01/03/2012	02/03/2012	100%	Analista Help Desk
6	* Coordinaciones previas a los trabajos de mantenimiento.	**6.1**	Elaborar lineamientos para los trabajos de mantenimiento a las PC's, Laptops, Impresoras, Otros	22/02/1900	09/03/2012	100%	Analista Help Desk
7	* Elaborar documentación técnica sobre función de los servidores	**7.1**	Elaborar instructivos técnicos para la manipulación de servidores (AS/400, Linux, otros)	10/02/2012	05/03/2012	100%	Jefe de Producción Coordinador I&N
8	* Capacitación a operadores en la estructura de Servidores	**8.1**	Capacitar a los Operadores en manipulación de Servidores (AS/400, Linux, otros)	06/03/2012	09/03/2012	100%	Coordinador I&N
9	* Actualización del MOF (detallando responsabilidades en Seg. Inf.)	**9.1**	Actualización de las responsabilidades MOF	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
10	* Asignar personal capacitado para el centro de Cómputo de contingencia	**10.1**	Evaluar personal para el Data Center de contingencia.	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo
		10.2	Asignar personal adecuado para el data center de contingencia	01/03/2012	30/03/2012	100%	Jf. Centro Cómputo
11	* Configurar claves para equipos BlackBerry	**11.1**	Elaborar instructivo de configuración de claves para bloqueo de equipos	01/03/2012	01/03/2012	100%	Administrador de Red

			BlackBerry				
12	* Contar con un stock mínimo de repuestos	**12.1**	Evaluar stock mínimo de Routers, Switch y Patch Panel	12/03/2012	14/03/2012	100%	Coordinador I&N
		12.2	Adquisición de stock de Routers, Switch y Patch Panel	15/03/2012	21/03/2012	100%	Coordinador I&N
		12.3	Inventariar equipos de comunicación	12/03/2012	23/03/2012	100%	Coordinador I&N
13	* Contar con un stock mínimo de repuestos y laptop	**13.1**	Evaluar stock mínimo repuestos de PC's y laptops	12/03/2012	14/03/2012	100%	Coordinador I&N
		13.2	Adquisición de stock de repuestos de PC's y laptops	12/03/2012	30/03/2012	100%	Coordinador I&N
		13.3	Inventariar de repuestos de PC's y laptops	30/03/2012	03/04/2012	100%	Coordinador I&N
14	* Implementar programa de mantenimiento preventivo de equipos.	**14.1**	Seleccionar equipos para el mantenimiento preventivo interno.	12/03/2012	16/03/2012	100%	Analista Help Desk
		14.2	Elaborar procedimiento para el Mantenimiento preventivo de equipos	19/03/2012	23/03/2012	100%	Analista Help Desk
		14.3	Elaborar programa de mantenimiento preventivo	26/03/2012	30/03/2012	100%	Analista Help Desk
15	* Corregir las instalaciones eléctricas	**15.1**	Detectar y reportar conexiones eléctricas inadecuadas	02/04/2012	06/04/2012	100%	Analista Help Desk
		15.2	Corregir instalaciones eléctricas inadecuadas	01/02/2012	01/03/2012	100%	Gerencia Administración
16	* Seguimiento a las garantías	**16.1**	Elaborar lineamientos para el seguimiento y control de garantías	20/02/2012	02/03/2012	100%	Jf. Centro Cómputo
17	* Mantener relaciones comerciales con proveedores estratégicos.	**17.1**	Elaborar de lista de proveedores, diferenciando los estratégicos	04/04/2012	10/04/2012	100%	Jefe de Producción Coordinador I&N
18	* Control diario del estado del antivirus y antispam	**18.1**	Elaborar lineamientos para el control y seguimiento diario del estado del antivirus y antispam	20/03/2012	21/03/2012	100%	Administrador de Red

		18.2	Elaborar bitácora de control de antivirus y antispam	22/03/2012	23/03/2012	100%	Administrador de Red
19	* Elaborar instructivos, políticas y procedimientos de operación y mantenimiento	**19.1**	Elaborar instructivos, políticas y procedimiento para la operación y mantenimiento de los HSM	05/03/2012	09/03/2012	100%	Jf. Centro Cómputo Jefe de Producción
		19.2	Elaborar instructivos, políticas y procedimiento para la operación y mantenimiento de la Central Telefónica	09/04/2012	20/04/2012	100%	Analista Help Desk
		19.3	Elaborar instructivos, políticas y procedimiento para la operación y mantenimiento de Firewall	01/04/2012	25/04/2012	100%	Coordinador I&N
		19.4	Elaborar instructivos para la operación y mantenimiento de antivirus y antispam	26/03/2012	29/03/2012	100%	Administrador de Red
		19.5	Elaborar instructivos para la operación y mantenimiento del servidor de correo	30/03/2012	04/04/2012	100%	Administrador de Red
		19.6	Elaborar instructivos para la operación y mantenimiento del directorio activo	05/04/2012	09/04/2012	100%	Administrador de Red
		19.7	Elaborar instructivos para la operación y mantenimiento del servidor de archivo	09/04/2012	13/04/2012	100%	Coordinador I&N Administrador de Red
		19.8	Elaborar instructivos para la operación y mantenimiento del Aranda	25/04/2012	01/05/2012	100%	Coordinador I&N
		19.9	Elaborar instructivos para la operación y mantenimiento del Servidor EPM	12/06/1900	23/04/2012	100%	Coordinador I&N
		19.10	Elaborar instructivos para la operación y mantenimiento del Servidor FTP	16/04/2012	23/04/2012	100%	Coordinador I&N Administrador de Red
		19.11	Elaborar instructivos para la operación y mantenimiento del Servidor IIS	16/04/2012	23/04/2012	100%	Coordinador I&N
		19.12	Elaborar instructivos para la operación y mantenimiento del Servidor MySQL	16/04/2012	23/04/2012	100%	Coordinador I&N

		19.13	Elaborar instructivos para la operación y mantenimiento del Servidor Card Perú al día	05/03/2012	12/03/2012	100%	Jefe de Producción
		19.14	Elaborar instructivos para la operación y mantenimiento del Servidor Travel PTA	16/04/2012	23/04/2012	100%	Coordinador I&N
		19.15	Elaborar instructivos para la operación y mantenimiento del Servidor Sybase	16/04/2012	23/04/2012	100%	Coordinador I&N
		19.16	Elaborar instructivos para la operación y mantenimiento del Servidor Drupal / Jbos	16/04/2012	23/04/2012	100%	Coordinador I&N
		19.17	Elaborar instructivos para la operación y mantenimiento del Servidor de Back UP	16/04/2012	23/04/2012	100%	Coordinador I&N
		19.18	Elaborar instructivos para la operación y mantenimiento del Servidor AS/400	01/04/2012	30/04/2012	100%	Jefe de Producción
		19.19	Elaborar instructivos para la operación y mantenimiento del Servidor Blackberry	23/04/2012	25/03/2012	100%	Administrador de Red
20	* Elaborar política de protección de equipos (PC's, laptops e Impresoras	**20.1**	Elaborar los política para la protección de PC's, laptops, impresoras, otros	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
21	* Habilitar restricciones en el dominio para prohibir desinstalación de programas.	**21.1**	Habilitar restricciones en el dominio para prohibir desinstalación de programas.	26/04/2012	26/04/2012	100%	Administrador de Red
22	* Habilitar el protector de pantalla automático	**22.1**	Habilitar el protector de pantalla automático	27/04/2012	27/04/2012	100%	Administrador de Red
23	* Habilitar restricciones de eliminación de iconos de escritorio.	**23.1**	Habilitar restricciones de eliminación de iconos de escritorio.	30/04/2012	30/04/2012	100%	Administrador de Red
24	* Eliminar usuarios genéricos	**24.1**	Identificar usuarios genéricos en todas las Sedes CP	01/05/2012	01/05/2012	100%	Jefe de Producción Administrador de Red
		24.2	Eliminar usuarios genéricos / Reasignar	01/05/2012	07/05/2012	100%	Administrador de Red

25	* Establecer un inventario actualizado de equipos (vida útil)	**25.1**	Definir vida útil de las PC's, laptops, servidores, UPS, otros	12/03/2012	23/03/2012	100%	Coordinador I&N
		25.2	Elaborar inventario actualizado de todos los equipos(incluir vida útil por equipo)	23/03/2012	23/04/2012	100%	Coordinador I&N
26	* Elaborar plan de renovación de equipos	**26.1**	Elaborar plan de renovación de equipos (PC's, laptops, UPS)	02/02/2012	22/02/2012	100%	Coordinador I&N
27	* Implementar nuevos Racks para servidores	**27.1**	Cotizar racks para servidores	01/03/2012	05/03/2012	100%	Coordinador I&N
		27.2	Remplazar racks antiguos	05/03/2012	05/04/2012	100%	Coordinador I&N
28	* Contar con un stock de contingencia de teléfono	**28.1**	Elaborar inventario de anexos y licencias AVAYA	23/04/2012	27/03/2012	100%	Analista Help Desk
		28.2	Sustentar compra de equipos IP y licencias AVAYA	30/04/2012	04/05/2012	100%	Analista Help Desk
		28.3	Adquirir stock de teléfonos y licencias	01/03/2012	30/03/2012	100%	Coordinador I&N
29	* Implementar solución automatizada para monitoreo de servidores * Implementar alertas sobre espacio en disco	**29.1**	Definir solución automatizada para el monitoreo de estado de servidores	01/03/2012	20/03/2012	100%	Coordinador I&N
		29.2	Implementación de Solución automatizada	20/03/2012	20/04/2012	100%	Coordinador I&N
		29.3	Capacitación en solución implementada	20/04/2012	04/05/2012	100%	Coordinador I&N
30	* Migrar Equipo Nortel a otra central telefónica	**30.1**	Dar de baja a Equipo Nortel	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo
		30.2	Adquisición de Nueva central telefónica	01/03/2012	30/03/2012	100%	Jf. Centro Cómputo
		30.3	Implementación de Nueva Central telefónica	30/03/2012	30/04/2012	100%	Jf. Centro Cómputo
31	* Implementar contingencia de central AVAYA (***)	**31.1**	Evaluar factibilidad de implementación de Contingencia de Central AVAYA	30/04/2012	04/05/2012	100%	Analista Help Desk
		31.2	Implementar contingencia AVAYA	15/02/2012	15/05/2012	100%	Analista Help Desk
32	* Implementar controles para visitas externas	**32.1**	Elaborar Check List de controles para visitas externas	01/02/2012	07/02/2012	100%	Gerencia Administración

		32.2	Implementar controles para visitas externas	07/02/2012	07/03/2012	100%	Gerencia Administración
		33.3	Elaborar procedimiento para la recepción de proveedores	07/03/2012	13/03/2012	100%	Gerencia Administración
33	* Implementar controles para prevenir el acceso físico del personal a lugares restringidos.	**33.1**	Elaborar Check List de controles para prevenir acceso físico de personal a lugares restringidos	01/02/2012	07/02/2012	100%	Gerencia Administración
		33.2	Implementar controles para para prevenir acceso físico de personal a lugares restringidos	07/02/2012	07/03/2012	100%	Gerencia Administración
		33.3	Elaborar lineamientos para ingreso a lugares restringidos	07/03/2012	13/03/2012	100%	Gerencia Administración
34	* Implementar controles/mecanismos de encriptación	**34.1**	Evaluar mecanismo de encriptación de datos para los equipos	20/02/2012	02/03/2012	100%	Jf. Centro Cómputo
		34.2	Implementar mecanismos de encriptación para las laptops, PC's, servidores, unidades de cinta	02/03/2012	02/04/2012	100%	Jf. Centro Cómputo
35	* Implementar control de claves a los servidores	**35.1**	Elaborar inventario de claves sensitivas	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		35.2	Asegurar ubicación de inventario	10/02/2012	10/02/2012	100%	Jf. Centro Cómputo
36	* Implementar control dual de clave maestra de servidores	**36.1**	Implementar control dual de clave maestra de servidores	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
37	* Renovar el sistema de control de accesos de producción.	**37.1**	Definir y cotizar sistema de control de accesos autorizado	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		37.2	Implementar nuevo sistema de control de accesos autorizado	10/02/2012	10/03/2012	100%	Jf. Centro Cómputo
38	* Cambiar la puerta de Data Center por una puerta de metal.	**38.1**	Definir y cotizar puerta adecuada para el Data Center	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		38.2	Implementar nueva puerta para Data Center	10/02/2012	10/03/2012	100%	Jf. Centro Cómputo
39	* Reubicar el Data Center / Mejorar la seguridad del Data Center (Principal y Contingencia)	**39.1**	Definir solución para la Seguridad del Data Center	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo

40	* Implementar procedimientos de cambios de configuración en servidores	**40.1**	Elaborar procedimiento de cambios de configuración de servidores	05/03/2012	09/03/2012	100%	Jf. Centro Cómputo
		40.2	Revisar y Aprobar procedimientos	12/03/2012	16/03/2012	100%	Jf. Centro Cómputo
41	* Implementar documentos para el retiro de equipos fuera de las instalaciones (políticas, formatos, procedimientos)	**41.1**	Elaborar procedimiento/formatos para el retiro de equipos físicos fuera de CP	05/03/2012	16/03/2012	100%	Jf. Centro Cómputo
		41.2	Revisar/Aprobar documentos para el retiro de equipos	05/03/2012	16/03/2012	100%	Jf. Centro Cómputo
42	* Implementar controles físicos de seguridad (laptops)	**42.1**	Implementar cables de seguridad para laptops	05/03/2012	16/03/2012	100%	Jf. Centro Cómputo
43	* Reubicar el servidor AVAYA	**43.1**	Elaborar análisis de factibilidad de reubicación del servidor AVAYA	05/03/2012	16/03/2012	100%	Jf. Centro Cómputo
		43.2	Planificar traslado de servidor AVAYA	19/03/2012	30/03/2012	100%	Jf. Centro Cómputo
		43.2	Traslado de servidor AVAYA	02/04/2012	13/04/2012	100%	Jf. Centro Cómputo
44	* Planificar los trabajos de mantenimiento de terceros	**44.1**	Elaborar inventario de contratos	06/02/2012	17/02/2012	100%	Jf. Centro Cómputo
		44.2	Programación de fechas de mantenimiento con terceros	19/02/2012	02/03/2012	100%	Jf. Centro Cómputo
45	* Implementar extintores apropiados para equipos electrónicos	**45.1**	Selección de tipos y cantidad de extintores	01/02/2012	07/02/2012	100%	Gerencia Administración
		45.2	Adquisición e implementación de extintores	07/02/2012	07/03/2012	100%	Gerencia Administración
46	* Capacitación en uso de extintores	**46.1**	Capacitación en uso de extintores	07/03/2012	13/03/2012	100%	Gerencia Administración
47	* Implementar detectores de aniego	**47.1**	Adquirir detectores de aniego	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo
		47.2	Definir zonas e Implementar detectores de aniego	05/02/2012	09/02/2012	100%	Jf. Centro Cómputo
48	* Implementar detectores de fuego	**48.1**	Adquirir detectores de fuego	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo
		48.2	Definir zonas e Implementar detectores de fuego	05/02/2012	09/02/2012	100%	Jf. Centro Cómputo
49	* Implementar extintores de Gas Halotron	**49.1**	Adquirir extintores de gases de Halotron y polvo químico	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo
		49.2	Implementar extintores especiales	05/02/2012	09/02/2012	100%	Jf. Centro Cómputo

50	* Implementar contingencia de servidores.	**50.1**	Adquisición de servidores físico, licencias, storage y software de replicación	01/02/2012	01/03/2012	100%	Coordinador I&N
		50.3	Instalación y configuración de equipos	01/03/2012	01/05/2012	100%	Coordinador I&N
		50.4	Ejecutar pruebas de contingencia	09/04/2012	30/04/2012	100%	Coordinador I&N
51	* Implementar aire acondicionado de precisión	**51.1**	Adquirir aire acondicionado de precisión	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo
		51.2	Implementar aire acondicionado de precisión	05/02/2012	09/02/2012	100%	Jf. Centro Cómputo
52	* Incluir equipos en el "proyecto de implementación UPS" para la oficina principal.	**52.1**	Incluir Equipos de comunicaciones y Central AVAYA con el UPS (proyecto)	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo
53	* Implementar contingencia de HSM ATALLA	**53.1**	Implementar desarrollo para la contingencia de HSM ATALLA	01/02/2012	01/03/2012	100%	Desarrollo
54	* Implementar racks de comunicaciones y muebles con seguridad (todas las sedes)	**54.1**	Definir cantidad, ubicación y tipo de racks de comunicaciones	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo/Coordinador I&N
		54.2	Adquirir racks de comunicaciones	01/03/2012	31/03/2012	100%	Jf. Centro Cómputo/Coordinador I&N
		54.3	Implementar muebles con seguridad a las sedes	01/04/2012	30/04/2012	100%	Gerencia Administración
		54.4	Implementar racks de comunicaciones en todas las Sedes	01/04/2012	30/04/2012	100%	Jf. Centro Cómputo/Coordinador I&N
55	* Implementar HA de Storage	**55.1**	Adquirir HA Storage	01/02/2012	31/03/2012	100%	Jf. Centro Cómputo/Coordinador I&N
		55.2	Implementar HA de Storage	01/04/2012	01/05/2012	100%	Jf. Centro Cómputo/Coordinador I&N

56	* Implementar mecanismos de control a los contratos de mantenimiento con terceros.	**56.1**	Elaborar lineamientos para el mantenimiento de equipos con terceros	06/02/2012	17/02/2012	100%	Jf. Centro Cómputo
57	* Implementar ubicaciones adecuadas para las cintas	**57.1**	Seleccionar ubicaciones seguras de almacenamiento	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		57.2	Almacenar cintas en zonas seguras	13/02/2012	24/02/2012	100%	Jf. Centro Cómputo
		57.3	Elaborar lineamientos para el almacenamiento de cintas.	27/02/2012	09/03/2012	100%	Jf. Centro Cómputo
58	* Implementar alertas automáticas UPS	**58.1**	Definir parámetros para alertas de UPS	06/02/2012	17/02/2012	100%	Jf. Centro Cómputo
		58.2	Implementar alertas ante fallas del UPS	17/02/2012	17/03/2012	100%	Jf. Centro Cómputo
59	* Implementar HA en firewall	**59.1**	Adquirir Switch	01/02/2012	01/03/2012	100%	Coordinador I&N
		59.2	Implementar HA de Firewall	01/03/2012	14/03/2012	100%	Coordinador I&N
60	* Implementar herramientas de monitoreo de tráfico de red	**60.1**	Adquirir herramienta de monitoreo de tráfico de red	01/02/2012	01/03/2012	100%	Coordinador I&N
		60.2	Implementar herramientas de monitoreo de tráfico de red	01/03/2012	14/03/2012	100%	Coordinador I&N
61	* Implementar HSM ATALLA	**61.1**	Implementar HSM ATALLA	01/03/2012	14/03/2012	100%	Desarrollo
		61.2	Desarrollar interface de comunicaciones	14/03/2012	14/05/2012	100%	Desarrollo
62	* Habilitar archivo físico para informes mensuales visados	**62.1**	Implementar archivo para informes mensuales	15/03/2012	15/03/2012	100%	Jf. Centro Cómputo
63	* Implementar IPS	**63.1**	Evaluación de soluciones de IPS	06/02/2012	17/02/2012	100%	Jf. Centro Cómputo
		63.2	Presentación y sustentación a Gerencia TI	20/02/2012	24/02/2012	100%	Jf. Centro Cómputo
		63.3	Adquirir IPS	24/02/2012	24/03/2012	100%	Jf. Centro Cómputo
		63.4	Implementación de IPS seleccionado	26/03/2012	06/04/2012	100%	Jf. Centro Cómputo/Coordinador I&N
64	* Implementar mecanismos de control para los usuarios maestros. (procedimientos, instructivos, formatos)	**64.1**	Elaborar inventario de usuarios maestros	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		64.2	Establecer control dual a usuarios maestros	10/02/2012	10/03/2012	100%	Jf. Centro Cómputo

65	* Implementar políticas y procedimientos para el uso de medios removibles	**65.1**	Elaboración lineamientos para el uso de medios removibles.	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		65.2	Revisión y aprobación de lineamientos	13/02/2012	17/02/2012	100%	I.G./G.M
66	* Implementar procedimiento para la baja de equipos.	**66.1**	Elaborar procedimiento de baja de equipos y eliminación de datos	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		66.2	Difundir procedimiento de baja de equipos	10/02/2012	10/02/2012	100%	Jf. Centro Cómputo
67	* Implementar procedimiento de control de claves a los Firewall	**67.1**	Elaborar inventario de usuarios maestros	13/02/2012	13/02/2012	100%	Jf. Centro Cómputo
		67.2	Establecer control dual a usuarios maestros	13/02/2012	13/03/2012	100%	Jf. Centro Cómputo
68	* Implementar detectores para el control de temperatura	**68.1**	Evaluación de tipos de detectores de T°.	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		68.2	Presentación y sustentación a Gerencia TI	13/02/2012	17/02/2012	100%	Jf. Centro Cómputo
		68.3	Adquirir detectores para el control de temperatura	17/02/2012	17/03/2012	100%	Jf. Centro Cómputo
		68.4	Implementación de detector de control de temperatura seleccionado	19/03/2012	23/03/2012	100%	Jf. Centro Cómputo
69	* Implementar aire acondicionado de precisión	**69.1**	Evaluación de tipos de aire acondicionado de precisión	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		69.2	Presentación y sustentación a Gerencia TI	13/02/2012	17/02/2012	100%	Jf. Centro Cómputo
		69.3	Adquirir aire acondicionado de precisión	17/02/2012	17/03/2012	100%	Jf. Centro Cómputo
		69.4	Implementación de aire acondicionado de precisión seleccionado	19/03/2012	23/03/2012	100%	Jf. Centro Cómputo
70	* Implementar deshumedecedor	**70.1**	Evaluación de tipos de deshumedecedor	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		70.2	Presentación y sustentación a Gerencia TI	13/02/2012	17/02/2012	100%	Jf. Centro Cómputo
		70.3	Adquirir deshumedecedor	17/02/2012	17/03/2012	100%	Jf. Centro Cómputo

		70.4	Implementación deshumedecedor seleccionado	19/03/2012	23/03/2012	100%	Jf. Centro Cómputo
71	* Implementar mecanismos de control a los contratos de mantenimiento con terceros.	**71.1**	Elaborar inventario de contratos	27/02/2012	09/03/2012	100%	Jf. Centro Cómputo
		71.2	Programación de fechas de mantenimiento con terceros	12/03/2012	23/03/2012	100%	Jf. Centro Cómputo
72	* Independizar UPS para protección exclusiva de los equipos de C. Cómputo.	**72.1**	Cotizar trabajo de circuito eléctrico independiente	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		72.2	Ejecutar trabajo circuito eléctrico	13/02/2012	17/02/2012	100%	Jf. Centro Cómputo
		72.3	Elaborar plan de pruebas de UPS	20/02/2012	24/02/2012	100%	Jf. Centro Cómputo
		72.4	Realizar pruebas de independización	27/02/2012	02/03/2012	100%	Jf. Centro Cómputo
73	* Implementar pruebas periódicas de restauración.	**73.1**	Elaborar cronograma de programación de pruebas de restauración	05/03/2012	16/03/2012	100%	Jefe de Producción
		73.2	Elaborar instructivos técnicos de pruebas	16/03/2012	09/04/2012	100%	Jefe de Producción
		73.3	Aperturar archivo físico de cronograma de programación	09/04/2012	13/04/2012	100%	Jefe de Producción
74	* Implementar política de equipo desatendido.	**74.1**	Elaborar Política de Equipo Desatendido	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		74.2	Revisión y Aprobación de Política	13/02/2012	17/02/2012	100%	Jf. Centro Cómputo
		74.3	Publicación de Política	17/02/2012	17/02/2012	100%	Jf. Centro Cómputo
75	* Habilitar el protector de pantalla automático	**75.1**	Aplicar directivas en servidor de protector de pantalla	07/05/2012	11/05/2012	100%	Administrador de Red
77	* Capacitación en uso de la bitácora de procesos	**77.1**	Preparar material de capacitación	01/02/2012	01/03/2012	100%	Jefe de Producción
		77.2	Programar capacitación a Operadores	01/03/2012	07/03/2012	100%	Jefe de Producción
		77.3	Ejecutar Capacitación	07/03/2012	21/03/2012	100%	Jefe de Producción
78	* Definir rol de DBA	**78.1**	Definir perfil de DBA	12/03/2012	16/03/2012	100%	Gerencia de Tecnología
		78.2	Seleccionar personal para cubrir rol	16/03/2012	16/04/2012	100%	Gerencia de Tecnología
79	* Definir roles para acceso a las BD y lineamientos para los cambios.	**79.1**	Elaborar mapa de accesos por roles	01/02/2012	20/02/2012	100%	DBA

80	* Implementar revisiones periódicas de accesos a BD.	**80.1**	Elaborar lineamientos para las revisiones de accesos a las BD	20/02/2012	09/03/2012	100%	DBA
81	* Implementar solución de control de acceso y monitoreo de BD	**81.1**	Cotizar solución de control de acceso y monitoreo de BD	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		81.2	Análisis Comparativo	13/02/2012	15/02/2012	100%	Jf. Centro Cómputo
		81.3	Elaboración de propuestas	15/02/2012	15/02/2012	100%	Jf. Centro Cómputo
		81.4	Presentación de propuestas	16/02/2012	21/02/2012	100%	Jf. Centro Cómputo
		81.5	Aprobación de presupuesto	22/02/2012	28/02/2012	100%	Jf. Centro Cómputo
		81.6	Envió de Orden de Compra	28/02/2012	28/02/2012	100%	Jf. Centro Cómputo
		81.7	Planificación e Implementación de solución	29/02/2012	06/03/2012	100%	Jf. Centro Cómputo
82	* Elaborar instrucciones técnicas de trabajo	**82.1**	Elaboración de instructivos de Produccion+HelpDesk+Infraestructura	01/03/2012	29/04/2012	100%	Jefe de Producción Coordinador I&N Analista Help Desk
		82.2	Publicación de instrucciones técnicas	30/04/2012	11/05/2012	100%	Jf. Centro Cómputo
83	* Escaneo de bitácora y almacenamientos por un año	**83.1**	Escaneo de Bitácora de Operación	01/02/2012	01/03/2012	100%	Jefe de Producción
		83.2	Almacenamiento en servidor de archivos	01/03/2012	07/03/2012	100%	Jefe de Producción
84	* Formalizar formato de bitácora	**84.1**	Elaborar Bitácora en PDF	01/03/2012	30/03/2012	100%	Jefe de Producción
		84.2	Aplicar seguridad a Bitácora	02/04/2012	06/04/2012	100%	Jefe de Producción
		84.3	Publicación de bitácora	09/04/2012	13/04/2012	100%	Jefe de Producción
85	* Implementar base de conocimientos en Aranda Help Desk	**85.1**	Capacitación en uso de base de conocimientos	09/02/2012	29/02/2012	100%	Coordinador I&N Analista Help Desk
		85.2	Incluir lineamientos en documentación de Help Desk	01/03/2012	30/03/2012	100%	Analista Help Desk
86	* Implementar de monitoreo de performance de BD	**86.1**	Planificación e Implementación de solución	09/03/2012	09/04/2012	100%	DBA
		86.2	Elaborar documentación para el control del monitoreo	27/02/2012	09/03/2012	100%	DBA
87	* Implementar procedimiento de afinamiento de BD	**87.1**	Implementar procedimiento de afinamiento de BD	09/03/2012	09/04/2012	100%	DBA
88	* Implementar informes mensuales	**88.1**	Coordinar reunión con Infraestructura	01/02/2012	15/02/2012	100%	Coordinador I&N

	sobre estado del antivirus	**88.2**	Definir procedimiento de trabajo	15/02/2012	01/03/2012	100%	Coordinador I&N
		88.3	Elaborar política y procedimiento de antivirus	01/03/2012	15/03/2012	100%	Coordinador I&N
89	* Habilitar archivo físico para informes mensuales de antivirus visados.	**89.1**	Solicitar archivo de palanca	01/03/2012	05/03/2012	100%	Coordinador I&N
		89.2	Implementar informes mensuales (incluir lineamientos de almacenamiento)	05/03/2012	26/03/2012	100%	Coordinador I&N
92	* Implementar mejoras en la certificación de aplicativos	**92.1**	Coordinar reunión con Desarrollo y Control de Calidad	20/02/2012	24/02/2012	100%	Jefe de Producción
		92.2	Definir plan de acción para el proceso de pase a producción	27/02/2012	09/03/2012	100%	Desarrollo
		92.3	Implementar mejoras al proceso de pases a producción	12/03/2012	23/03/2012	100%	Desarrollo
93	* Implementar plan de actualización de versiones	**93.1**	Elaborar inventario de software	01/02/2012	24/02/2012	100%	Coordinador I&N
		93.2	Programar reunión de coordinación para actualización de versiones de SW	27/02/2012	09/03/2012	100%	Coordinador I&N
		93.2	Definición de plan de actualización de versiones ANUAL 2012-2013	09/03/2012	23/03/2012	100%	Coordinador I&N
94	* Implementar un plan de actualización de parches anual	**94.1**	Elaborar inventario de software	01/02/2012	15/02/2012	100%	Coordinador I&N
		94.2	Definición de plan de actualización de parches ANUAL 2012-2013	15/02/2012	01/03/2012	100%	Coordinador I&N
95	* Implementar control de claves a las BD	**95.1**	Inventario de usuarios sensitivos	01/02/2012	01/03/2012	100%	Jefe de Producción
		95.2	Implementar control dual a las claves de BD	01/03/2012	30/03/2012	100%	Jefe de Producción
96	* Implementar soluciones de encriptación y enmascaramiento de BD	**96.1**	Cotizar solución de encriptación y enmascaramiento	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		96.2	Análisis Comparativo	13/02/2012	15/02/2012	100%	Jf. Centro Cómputo
		96.3	Elaboración de propuestas	15/02/2012	15/02/2012	100%	Jf. Centro Cómputo
		96.4	Presentación de propuestas	16/02/2012	21/02/2012	100%	Jf. Centro Cómputo
		96.5	Aprobación de presupuesto	22/02/2012	28/02/2012	100%	Jf. Centro Cómputo
		96.6	Envió de Orden de Compra	28/02/2012	28/02/2012	100%	Jf. Centro Cómputo

		96.7	Planificación e Implementación de solución	29/02/2012	06/03/2012	100%	Jf. Centro Cómputo
98	* Mejorar el proceso de pase a producción	**98.1**	Coordinar reunión con Desarrollo y Control de Calidad	06/02/2012	06/10/2012	100%	Jefe de Producción
		98.2	Definir plan de acción para el proceso de pase a producción	13/02/2012	24/02/2012	100%	Jefe de Producción
		98.3	Implementar mejoras al proceso de pases a producción	24/02/2012	24/03/2012	100%	Jefe de Producción
99	*Mejorar el sistema de pases a producción	**99.1**	Elaborar nuevas funcionalidades en sistema	01/03/2012	30/03/2012	100%	Desarrollo
		99.2	Ingresar requerimiento de modificación al sistema	02/04/2012	06/04/2012	100%	Jefe de Producción
		99.3	Modificación del sistema de pase a producción	30/03/2012	12/04/2012	100%	Desarrollo
		99.4	Implementación en producción	12/04/2012	23/04/2012	100%	Desarrollo
100	* Renovación tecnológica	**100.1**	Programación anual de renovación tecnológica	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
102	* Digitalizar contratos físicas	**102.1**	Inventario de contratos	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
		102.2	Digitalización de contratos	13/02/2012	17/02/2012	100%	Jf. Centro Cómputo
103	* Implementar mecanismos de control para renovación de contratos	**103.1**	Elaboración de inventario de contratos y fechas de renovación	20/02/2012	24/02/2012	100%	Jf. Centro Cómputo
		103.2	Establecer mecanismos de alertas de fechas de renovación	27/02/2012	02/03/2012	100%	Jf. Centro Cómputo
104	* Elaborar inventario de servicios FTP (información sobre uso, datos de acceso)	**104.1**	Inventario de servicios FTP	06/02/2012	17/02/2012	100%	Jefe de Producción
		104.2	Alojar archivo en SharePoint	20/02/2012	02/03/2012	100%	Jefe de Producción
105	* Implementar control de claves para FTP	**105.1**	Inventario de usuarios sensitivos	01/02/2012	01/03/2012	100%	Jefe de Producción
106	* Elaborar lista de contactos para los Servicios En Línea y Lotes	**106.1**	Elaborar lista de contactos	06/02/2012	17/02/2012	100%	Jefe de Producción
		106.2	Alojar archivo en SharePoint	20/02/2012	02/03/2012	100%	Jefe de Producción

107	* Elaborar procedimientos de comunicaciones para los servicios En Línea y Lotes	**107.1**	Elaborar plantilla de correo de comunicación interna por cambios/mantenimientos de los servicios de terceros (DCI, DISCOVER, PULSE, MC, INTERBANK, etc.)	06/02/2012	17/02/2012	100%	Jefe de Producción
		107.2	Elaboración procedimiento de comunicación	20/02/2012	02/03/2012	100%	Jefe de Producción
110	* Implementar mecanismos de control para renovación de licencias.	**110.1**	Elaboración de inventario de renovación de licencias	20/02/2012	24/02/2012	100%	Jf. Centro Cómputo
		110.2	Establecer mecanismos de alertas de fechas de renovación	27/02/2012	02/03/2012	100%	Jf. Centro Cómputo
111	* Elaborar plan de capacitación anual (nuevas tecnologías)	**111.1**	Programación anual de capacitaciones	06/02/2012	10/02/2012	100%	Jf. Centro Cómputo
113	* Elaborar y difundir MOFs	**113.1**	Elaborar/Actualizar MOF por cargos	01/02/2012	01/03/2012	100%	Jf. Centro Cómputo
		113.2	Revisión y aprobación final	05/03/2012	09/03/2012	100%	Jf. Centro Cómputo
114	* Mantener actualizado la información la documentación.	**114.1**	Programación anual de actualización de documentación	05/03/2012	09/03/2012	100%	Jf. Centro Cómputo
116	* Implementar compromiso de confidencialidad de información	**116.1**	Elaborar compromiso en coordinación con SubGte. De Administración y legal	20/02/2012	24/02/2012	100%	Gerencia Administración
119	* Implementar mecanismos de control y seguimiento de la ejecución de los procesos	**119.1**	Convocar a personal involucrado en los procesos CP	06/02/2012	17/02/2012	100%	Jefe de Producción
		119.2	Sustentación de mecanismos de control	20/02/2012	02/03/2012	100%	Jefe de Producción
		119.3	Asignación de nuevas funciones de control	05/03/2012	09/03/2012	100%	Jefe de Producción
		119.4	Actualización de Bitácora de Operación	12/03/2012	23/03/2012	100%	Jefe de Producción
		119.5	Implementación de controles	23/03/2012	23/04/2012	100%	Jefe de Producción
120	* Implementar mecanismos de consistencia de la información para los servicios en lotes	**120.1**	Elaborar relación de archivos y procesos a consistenciar	06/02/2012	17/02/2012	100%	Jefe de Producción
		120.2	Reunión de análisis de factibilidad con Jefe de Desarrollo	20/02/2012	02/03/2012	100%	Jefe de Producción
		120.3	Ingresar requerimiento a Desarrollo	05/03/2012	09/03/2012	100%	Jefe de Producción

		120.4	Actualizar Bitácora de Operación	12/03/2012	23/03/2012	100%	Jefe de Producción
		120.5	Implementación de consistencias	23/03/2012	23/04/2012	100%	Jefe de Producción
121	* Implementar medios de transmisión seguros (FTPS)	**121.1**	Elaborar relación de archivos intercambiados con entidades externas	06/02/2012	17/02/2012	100%	Jefe de Producción
		121.2	Configurar servidores SFTP por entidad	20/02/2012	02/03/2012	100%	Jefe de Producción
		121.3	Actualizar Bitácora de Operación	05/03/2012	09/03/2012	100%	Jefe de Producción
		121.4	Comunicar nuevo esquema de intercambio con entidades	12/03/2012	23/03/2012	100%	Jefe de Producción
		121.5	Planificación e Implementación de servidores SFTP	23/03/2012	23/04/2012	100%	Jefe de Producción
122	* Implementar monitoreo de red	**122.1**	Cotizar solución de monitoreo de red	01/02/2012	01/03/2012	100%	Coordinador I&N
		122.2	Análisis Comparativo	01/03/2012	07/03/2012	100%	Coordinador I&N
		122.3	Elaboración de propuestas	07/03/2012	09/03/2012	100%	Coordinador I&N
		122.4	Presentación de propuestas	09/03/2012	09/03/2012	100%	Coordinador I&N
		122.5	Aprobación de presupuesto	12/03/2012	16/03/2012	100%	Coordinador I&N
		122.6	Envió de Orden de Compra	16/03/2012	16/03/2012	100%	Coordinador I&N
		122.7	Planificación e Implementación de solución	19/03/2012	23/03/2012	100%	Coordinador I&N
123	* Implementar contingencia de internet	**123.1**	Cotizar servicio de internet con contingencia	01/02/2012	15/02/2012	100%	Coordinador I&N
		123.2	Análisis Comparativo	15/02/2012	21/02/2012	100%	Coordinador I&N
		123.3	Elaboración de propuestas	21/02/2012	23/02/2012	100%	Coordinador I&N
		123.4	Presentación de propuestas	23/02/2012	23/02/2012	100%	Coordinador I&N
		123.5	Aprobación de presupuesto	24/02/2012	01/03/2012	100%	Coordinador I&N
		123.6	Envió de Orden de Compra	01/03/2012	01/03/2012	100%	Coordinador I&N
		123.7	Planificación e Implementación del servicio de internet de contingencia	02/03/2012	08/03/2012	100%	Coordinador I&N

Cuadro 3.26: Plan de tratamiento de riesgos de departamento de centro de cómputo [61]

D) Plan de tratamiento de riesgos – Brecha circular N° G-140

PLAN TRABAJO PARA EL CUMPLIMIENTO CON LA CIRCULAR G-140 (SBS)								
Nro.	**G-140**	**MECANISMOS DE PROTECCIÓN**		**Plazo**		**Avance %**	**Responsables**	**Tiempos**
				Inicio	**Fin**			
1	Generalidades	Definición y difusión de una política	Revisión/Aprobación de Política de SGSI	02/02/2012	02/02/2012	100%	A. G. procesos	1hs
			Publicación de la Política del SGSI	02/02/2012	02/02/2012	100%	A. G. procesos	1hs
		Metodología de Gestión de Riesgos	Revisión del Metodología de Gestión de Riesgos	02/02/2012	02/02/2012	100%	A. G. procesos	1hs
			Homologación de metodología con G. Riesgo Operacional	03/02/2012	03/02/2012	100%	A. G. procesos	1ds
		Mantenimiento de Registros	Adecuación de Procedimiento de Control de Registros	06/02/2012	06/02/2012	100%	A. G. procesos	1hs
		Asegurar el cumplimiento de la políticas	Identificar mecanismos para el cumplimiento de las políticas	06/02/2012	07/02/2012	100%	A. G. procesos	1ds
			Implementar mecanismos de cumplimiento	07/02/2012	09/02/2012	100%	A. G. procesos	3ds
		Método para la evaluación de incidentes de seguridad / acciones	Elaborar metodología para la evaluación de incidentes de seguridad y acciones inmediatas	13/02/2012	14/02/2012	100%	A. G. procesos	2ds
			Revisión / Aprobación de metodología	15/02/2012	15/02/2012	100%	A. G. procesos	1ds

[61] Elaboración: los autores.

2	**Seguridad Lógica**	Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.	Elaborar procedimiento y formatos para la Gestión de Accesos	15/02/2012	17/02/2012	100%	Jf. Centro Cómputo	3ds
			Revisión/Aprobación de procedimiento y formatos	20/02/2012	20/02/2012	100%	Jf. Centro Cómputo	1ds
		Revisiones periódicas sobre los derechos concedidos a los usuarios.	Elaborar lineamientos para las revisiones periódicas sobre los derechos concedidos	21/02/2012	21/02/2012	100%	Jf. Centro Cómputo	1ds
		Controles especiales sobre utilidades del sistema y herramientas de auditoría.	Identificar pistas de auditoria	22/02/2012	22/02/2012	100%	Auditor Interno	1ds
			Adecuar controles para el cumplimiento de las pistas de auditoria	22/02/2012	24/02/2012	100%	Auditor Interno	3ds
		Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.	Definir mecanismos para el seguimientos de las actividades no autorizadas	27/02/2012	27/02/2012	100%	Jf. Centro Cómputo	2hs
		Controles especiales sobre usuarios remotos y computación móvil.	Revisar y difundir procedimiento para el acceso de usuarios remotos	27/02/2012	27/02/2012	100%	Jf. Centro Cómputo	3hs
3	**Seguridad de Personal**	Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.	Definir criterios para el control disciplinario	28/02/2012	07/03/2012	100%	Gerente de RR.HH	7ds
			Elaborar el proceso disciplinario para el incumplimiento de la seguridad de información	08/03/2012	09/03/2012	100%	Gerente de RR.HH	2ds
			Revisión con el área legal / Difusión	12/03/2012	12/03/2012	100%	Gerente Legal	1ds
		Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la	Elaborar procedimientos/formatos para la revocación de derechos y devolución de activos en caso de cese de personal	13/03/2012	14/03/2012	100%	Jf. Centro Cómputo	2ds

		revocación de los derechos de acceso y la devolución de activos.	Revisión/Aprobación/Difusión de procedimientos y formatos	15/03/2012	15/03/2012	100%	Jf. Centro Cómputo	1ds
4	**Inventario de Activos y Clasificación de la Información**	Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.	Definir responsabilidades por Dpto. para el mantenimiento del inventario de activos y gestión de riesgos	12/03/2012	20/03/2012	100%	Gerente Tecnología	7ds
		Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.	Adecuación del Manual DCP-GP-M-001 Guía para el Análisis Y Gestión de Riesgos A.I	21/03/2012	22/03/2012	100%	A. G. procesos	2ds
5	**Administración de las operaciones y comunicaciones**	Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.	Definir controles para los cambios que se realizan en los servicios de tecnología.	26/03/2012	27/03/2012	100%	Adm. De Red	2ds
		Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.	Elaborar lineamientos sobre el acceso a las redes	28/03/2012	30/03/2012	100%	Adm. De Red	3ds
			Implementar controles para acceso a las redes	02/04/2012	03/04/2012	100%	Adm. De Red	2ds
		Seguridad sobre el intercambio de la información, incluido el correo electrónico.	Implementar un sistema de intercambio de información protegido	09/04/2012	20/04/2012	100%	Adm. De Red	10ds

		Seguridad sobre canales electrónicos.	Implementar seguridad sobre canales electrónicos.	23/04/2012	25/04/2012	100%	Adm. De Red	3ds
		Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.	Identificación e registros obligatorios para la auditoria y monitoreo de sistemas	26/04/2012	27/04/2012	100%	Auditor Interno	2ds
6	**Adquisición, desarrollo y mantenimiento de sistemas informáticos**	Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.	Realizar inventario de los sistemas existentes en la empresa	02/02/2012	02/02/2012	100%	Jf. Desarrollo	1ds
			Identificar las vulnerabilidades técnicas de los sistemas críticos.	03/02/2012	05/02/2012	100%	Jf. Desarrollo	3ds
7	**Gestión de Incidentes de Seguridad de Información**	Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.	Elaborar lineamientos para el reporte de la identificación de los incidentes de seguridad y vulnerabilidades	26/03/2012	28/03/2012	100%	A. G. Procesos	3ds
			Revisión y Aprobación de lineamientos	29/03/2012	29/03/2012	100%	A. G. Procesos	1ds
		Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.	Elaborar lineamientos para la respuesta ante un incidentes de seguridad y o una vulnerabilidades detectados.	02/04/2012	04/04/2012	100%	A. G. Procesos	3ds
			Revisión y Aprobación de lineamientos	05/04/2012	05/04/2012	100%	A. G. Procesos	1ds

Cuadro 3.27: Plan de tratamiento de riesgos – brecha circular N° G-140 [62]

[62] Elaboración: los autores.

CAPÍTULO IV
PRUEBAS Y RESULTADOS

4.1 Análisis de brechas post

El siguiente cuadro muestra el análisis de brechas realizado después de la implementación de controles de análisis de riesgos.

Ítem	Requisitos circular G-140	Cumple	Nivel cumplimiento	
Generalidades				
1	Definición y difusión de una política	**SÍ**	50%	
2	Metodología de gestión de riesgos	**SÍ**	80%	
3	Mantenimiento de registros	**SÍ**	50%	
4	Estructura organizacional definida y difundida	**SÍ**	100%	
5	Asegurar el cumplimiento de la política	**NO**	0%	**60%**
6	Monitoreo de la implementación de controles	**SÍ**	100%	
7	Método para la concientización y entrenamiento del personal	**SÍ**	100%	
8	Método para la evaluación de incidentes de seguridad / acciones	**NO**	0%	
Seguridad lógica				
9	Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.	**SÍ**	50%	
10	Revisiones periódicas sobre los derechos concedidos a los usuarios.	**SÍ**	50%	
11	Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.	**SÍ**	100%	**42%**
12	Controles especiales sobre utilidades del sistema y herramientas de auditoría.	**NO**	0%	

13	Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.	NO	0%	
14	Controles especiales sobre usuarios remotos y computación móvil.	SÍ	50%	
Seguridad de personal				
15	Definición de roles y responsabilidades establecidos sobre la seguridad de información.	SÍ	100%	**66%**
16	Verificación de antecedentes, de conformidad con la legislación laboral vigente.	SÍ	100%	
17	Concientización y entrenamiento.	SÍ	100%	
18	Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.	NO	0%	
19	Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.	NO	0%	
Seguridad física y ambiental				
20	Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.	SÍ	80%	**80%**
21	Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.	SÍ	80%	
Inventario de activos y clasificación de la información				
22	Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.	SÍ	80%	**80%**
23	Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.	SÍ	80%	
Administración de las operaciones y				

comunicaciones				
24	Procedimientos documentados para la operación de los sistemas.	**SÍ**	80%	**58%**
25	Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.	**NO**	0%	
26	Separación de funciones para reducir el riesgo de error o fraude.	**SÍ**	80%	
27	Separación de los ambientes de desarrollo, pruebas y producción.	**SÍ**	100%	
28	Monitoreo del servicio dado por terceras partes.	**SÍ**	100%	
29	Administración de la capacidad de procesamiento.	**SÍ**	70%	
30	Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.	**SÍ**	100%	
31	Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.	**SÍ**	30%	
32	Seguridad sobre el intercambio de la información, incluido el correo electrónico.	**SÍ**	25%	
33	Seguridad sobre canales electrónicos.	**SÍ**	50%	
34	Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.	**NO**	0%	
Adquisición, desarrollo y mantenimiento de sistemas informáticos				
35	Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.	**SÍ**	100%	**75%**
36	Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.	**SÍ**	100%	
37	Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.	**SÍ**	100%	
38	Controlar el acceso a las librerías de programas fuente.	**SÍ**	100%	

39	Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.	**SÍ**	50%	
40	Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.	**NO**	0%	
Procedimientos de respaldo				
41	Procedimientos de respaldo regular y periódicamente validado. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la empresa.	**SÍ**	100%	**100%**
42	Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento.	**SÍ**	100%	
Gestión de incidentes de seguridad de información				
43	Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.	**NO**	0%	**40%**
44	Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.	**SÍ**	80%	

Cuadro 3.28: Análisis de brechas POST [63]

[63] Elaboración: los autores.

4.1.1 Resultado después de implementar los controles del análisis de Riesgos

Antes:
Ver 2.2.2.3

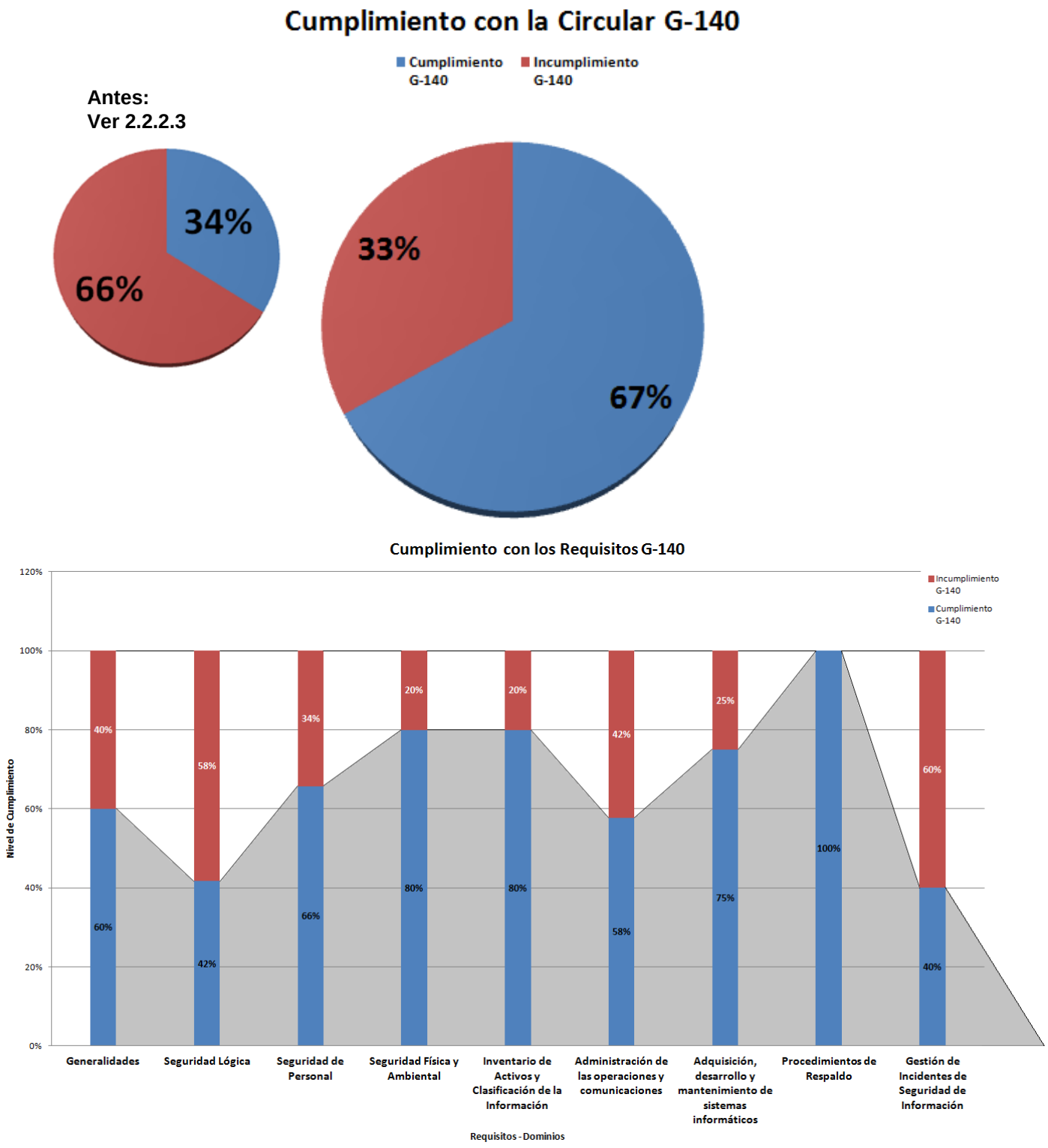
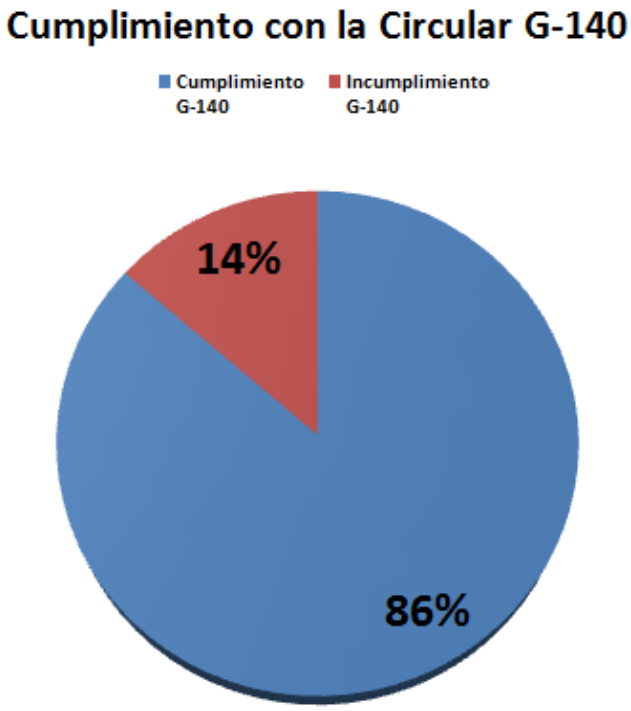


Gráfico 4.1: Resultado después de aplicar controles de análisis de riesgos [64]

[64] Elaboración: los autores.

4.1.2 Resultado después de implementar los controles de la circular g-140



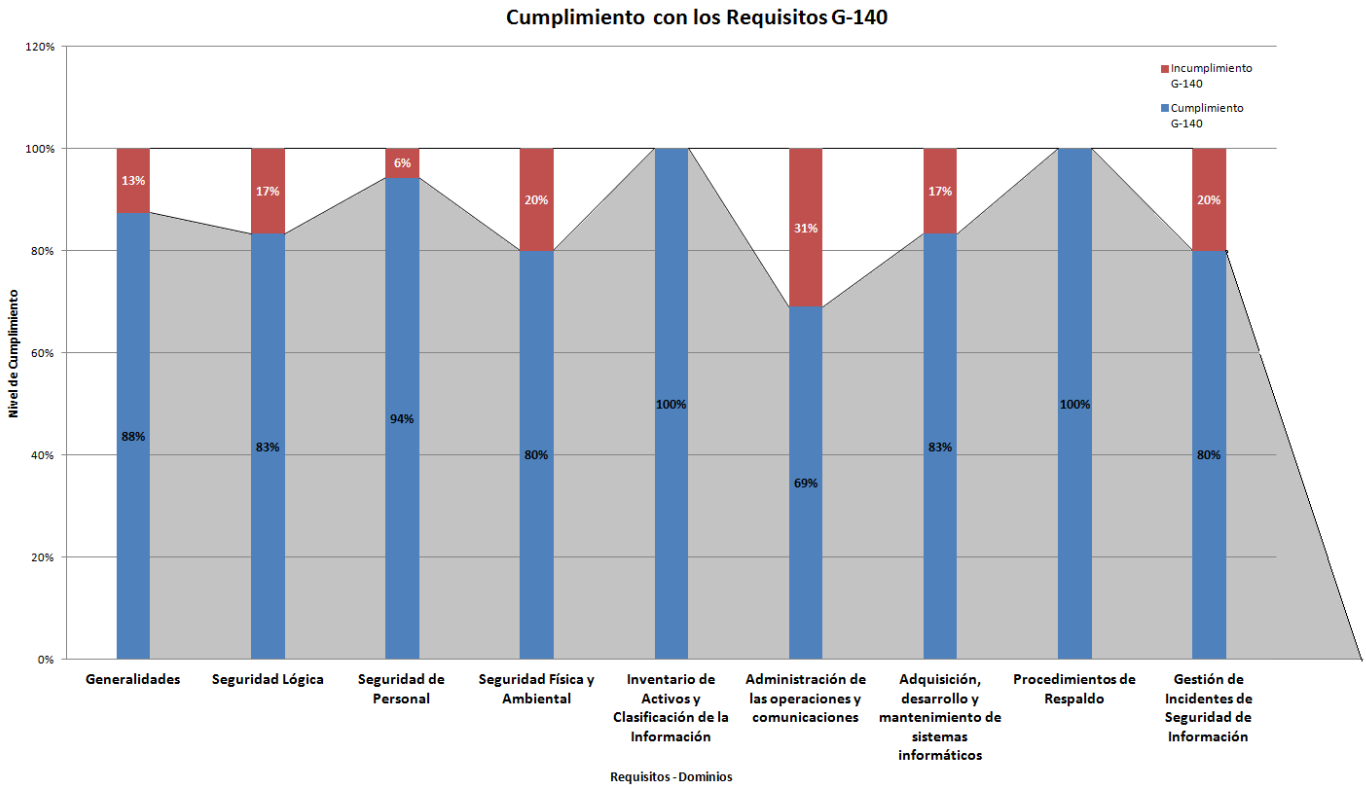


Gráfico 4.1: Resultado después de aplicar controles de circular N° G-140 [65]

[65] Elaboración: los autores.

4.2 Despliegue de indicadores

4.2.1 Objetivos VS Indicadores

Objetivos	Indicadores (%)	Fórmula	Meta
Implementar una política de seguridad de información que sea desplegada a todos los colaboradores, proveedores y terceros involucrados en los procesos de tecnología.	Colaboradores que conocen la política de seguridad de información	Nro. Colabor. Conocen / Nro. Total colaboradores	**100%**
	Colaboradores que cumplen de la política de seguridad de información	Nro. Colabor. Cumplen / Nro. Total colaboradores	**80%**
Gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de información, para reducirlos en un 80%.	Incidentes reportados adecuadamente	Nro. Incidentes reportados ad. / Nro. Total incidentes	**80%**
	Vulnerabilidades reportadas adecuadamente	Nro. Vulnerab. Reportados ad. / Nro. Total vulnerabilidades	**80%**
	Incidentes atendidos oportunamente	Nro. Incidentes atendidos / Nro. Total incidentes	**95%**
	Vulnerabilidades atendidos oportunamente	Nro. Vulnerab. Atendidos / Nro. Total vulnerabilidades	**85%**
Desplegar las medidas de seguridad para gestionar los riesgos y ejecutar controles de tratamiento de riesgos, para reducir el 90% de los riesgos a niveles aceptables.	Activos de información sin mecanismos de control	Nro. Activos sin control / Nro. Total de activos	**0%**
	Riesgos con nivel de tolerancia "No tolerables"	Nro. Riesgos NT. / Nro. Total de riesgos	**0%**
	Riesgos con nivel de tolerancia "Totalmente tolerables"	Nro. Riesgos TT / Nro. Total de riesgos	**65%**

Formación y concientización al 100% de los colaboradores involucrados en los procesos de tecnología, en temas de seguridad de información.	Colaboradores capacitados/concientizados	Nro. Colaboradores capaci. Nro. Total de colaboradores	**100%**
	Colaboradores capacitados/concientizados aprobados > 13	Nro. Aprobados > 13 Nro. Total de capacitados	**90%**
Cumplimiento de la legislación vigente sobre información personal, propiedad intelectual y otras.	Cumplimiento de requisitos reglamentarios	Análisis de Brechas	**90%**
Gestionar y controlar el 100% de los documentos del SGSI.	Procedimientos necesarios SGSI documentados/ estandarizados/ Difundidos	Nro. Procedimientos DED Nro. Total de requisitos	**90%**
	Cumplimiento de los procedimientos SGSI documentados/ estandarizados/ Difundidos	Nro. Cumplimiento Proced Nro. Total de Proced.	**90%**

Cuadro 3.29: Objetivos VS indicadores [66]

[66] Elaboración: los autores.

4.2.2 Resultado de indicadores antes vs después

Indicadores (%)	Antes		Después	
Colaboradores que conocen la política de seguridad de información	5/52	**10%**	52/52	**100%**
Colaboradores que cumplen de la política de seguridad de información	5/52	**10%**	40/52	**77%**
Incidentes reportados adecuadamente (1 mes)	494/918	**54%**	756/871	**87%**
Vulnerabilidades reportadas adecuadamente (1 mes)	15/67	**22%**	18/23	**78%**
Incidentes atendidos oportunamente (1 mes)	813/918	**88%**	852/871	**98%**
Vulnerabilidades atendidos oportunamente (1 mes)	50/67	**75%**	18/23	**78%**
Activos de información sin mecanismos de control	39/88	**44%**	88/88	**0%**
Riesgos con nivel de tolerancia "No tolerables"	12/268	**4.5%**	0/268	**0%**
Riesgos con nivel de tolerancia "Totalmente tolerables"	87/268	**32.5%**	207/268	**77%**
Colaboradores capacitados/concientizados en SI	5/52	**10%**	52/52	**100%**
Colaboradores capacitados/concientizados aprobados > 13	5/52	**10%**	38/52	**73%**
Cumplimiento de requisitos reglamentarios	Brecha Pre	**34%**	Brecha Post	**86%**
Procedimientos necesarios SGSI documentados/ estandarizados/ Difundidos *	3/15	**20%**	15/15	**100%**
Cumplimiento de los procedimientos SGSI documentados/ estandarizados/ Difundidos	2/3	**67%**	12/15	**80%**

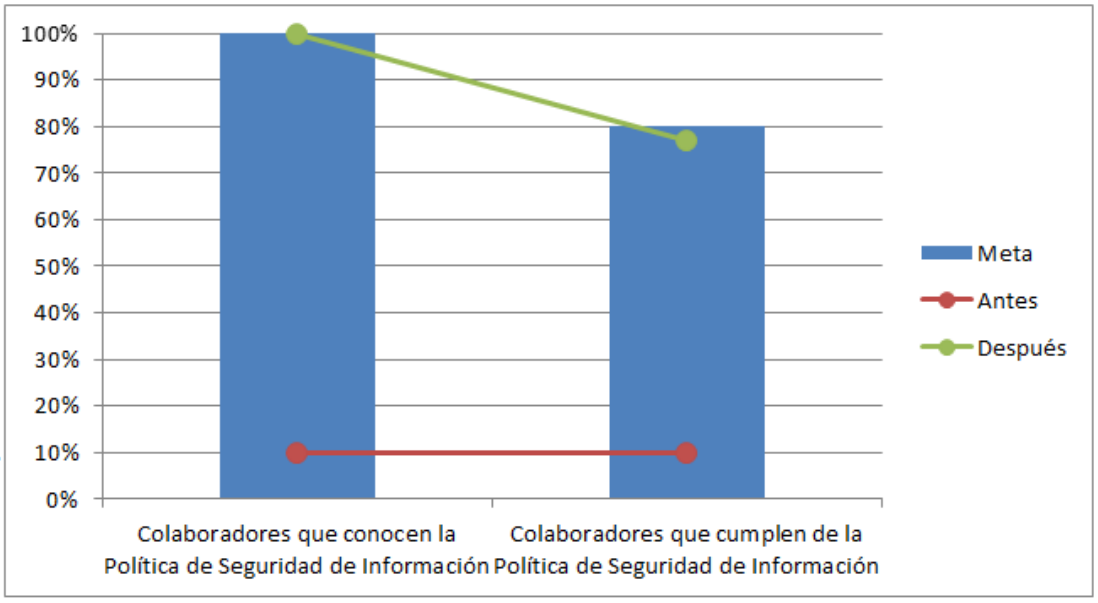
Cuadro 3.30: Resultado de indicadores antes VS después [67]

* Los documentos necesarios SGSI son: política SGSI, manual SGSI, procedimiento de gestión de riesgos, procedimiento de gestión de incidentes y vulnerabilidades, procedimiento de gestión de usuarios, procedimiento de control de accesos, procedimientos disciplinarios de seguridad, procedimiento para cese de personal, procedimiento para ingreso de personal, política sobre seguridad física y ambiental, procedimientos de la operación de sistemas, procedimientos para el monitoreo del trabajo de terceros, políticas sobre la gestión de la capacidad de procesamiento, procedimiento para la adquisición, desarrollo y mantenimiento de sistemas, procedimientos de respaldo.

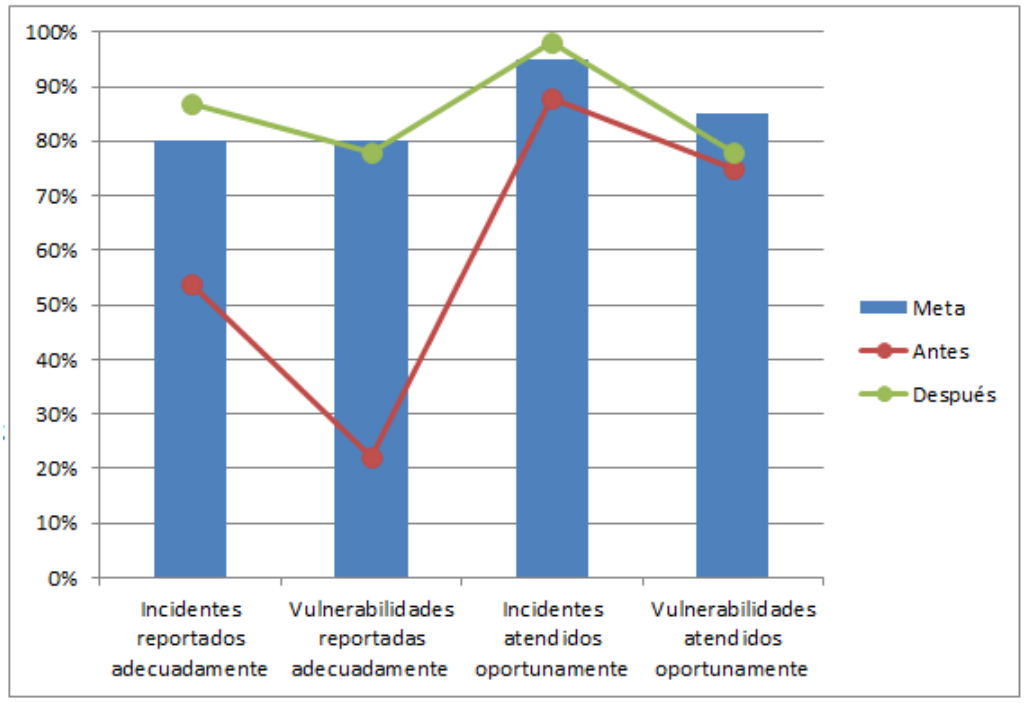
[67] Elaboración: los autores.

4.2.3 Gráficos de mejora de indicadores [68]

- **Objetivo 1:** Implementar una política de seguridad de información que sea entendida, cumplida e interiorizada por el 100% de los colaboradores involucrado en los procesos de Tecnología

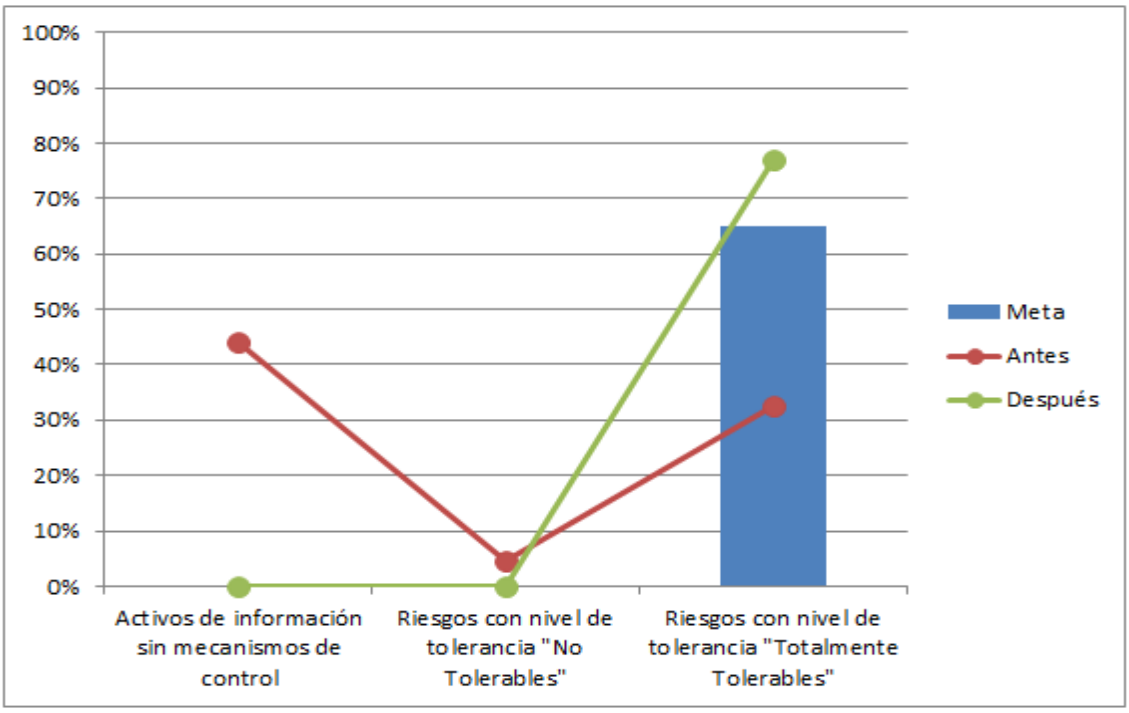


- **Objetivo 2:** Gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de información para reducir los impactos en un 80%.

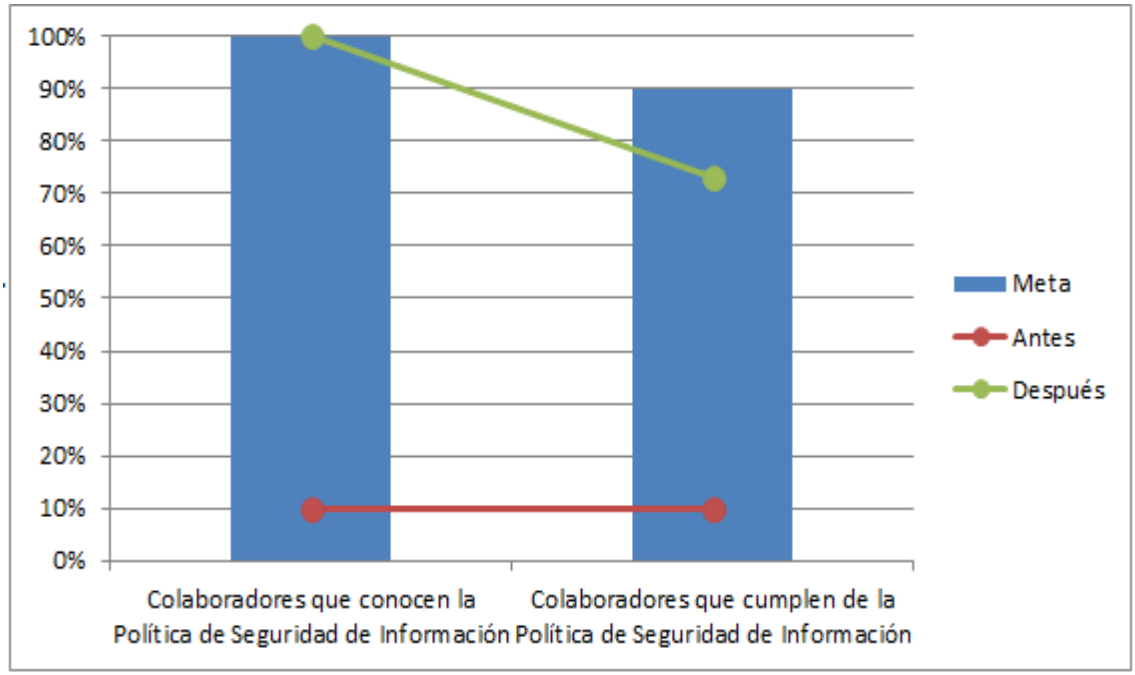


[68] Fuente: Gráficos elaborados por el equipo de proyecto para mostrar las mejores obtenidas basados en los indicadores luego de implementar los controles propuestos.

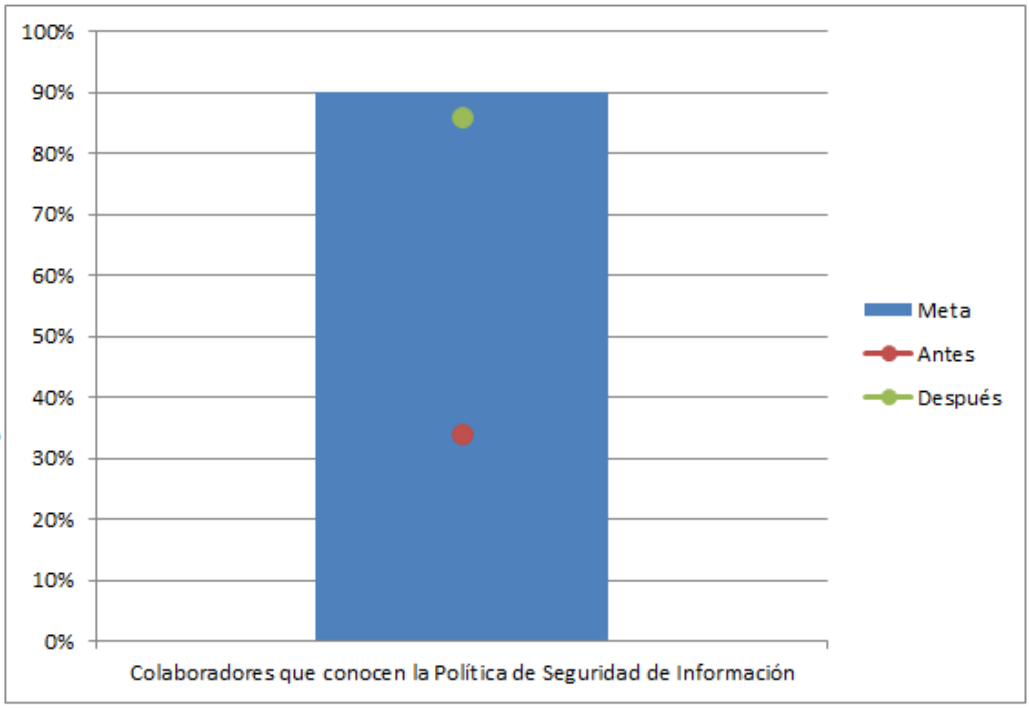
➢ **Objetivo 3:** Desplegar las medidas de seguridad para gestionar los riesgos y ejecutar el plan de tratamiento de riesgos planteado para reducir el 90% de los riesgos a niveles aceptables.



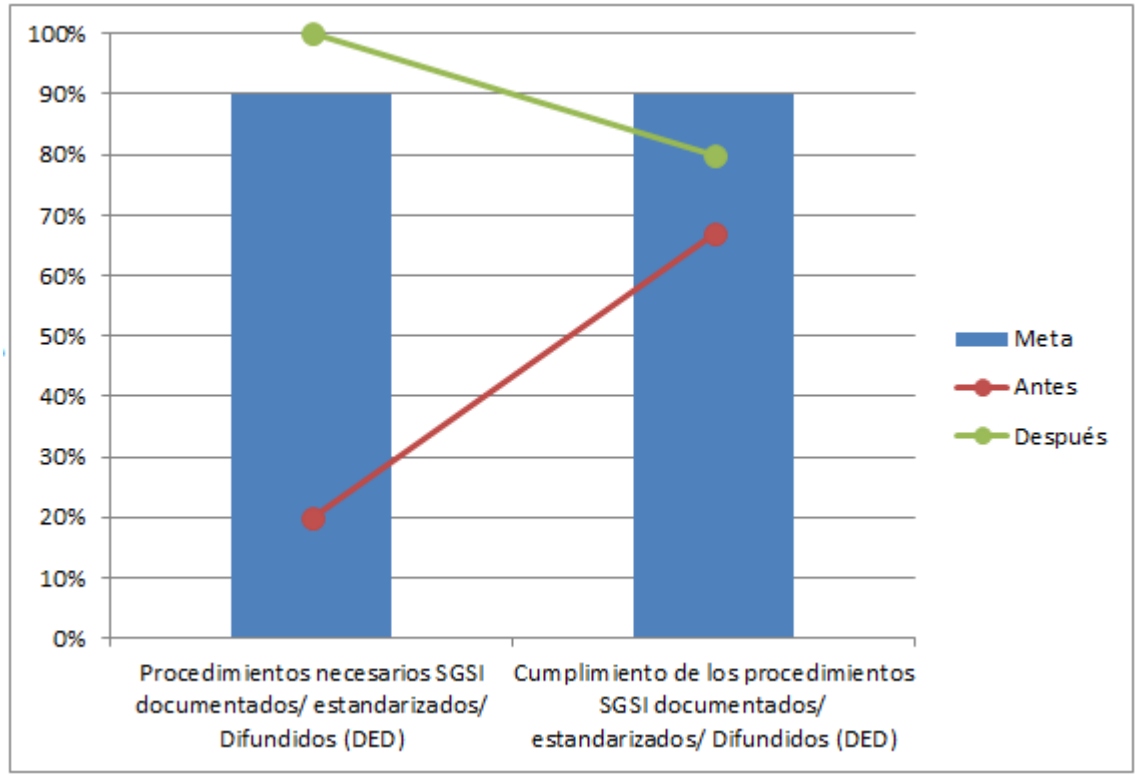
➢ **Objetivo 4:** Formación y concientización al 100% de los colaboradores involucrados en los procesos de tecnología en temas de seguridad de información.



➢ **Objetivo 5:** Cumplimiento de la legislación vigente sobre información personal, propiedad intelectual y otras.



➢ **Objetivo 6:** Gestionar y controlar el 100% de los documentos del SGSI.



4.3 Beneficios obtenidos

- Provee a la gerencia dirección y apoyo para la seguridad de la información.
- Ayuda a identificar los activos de información y a protegerlos adecuadamente.
- Enfoque sistemático para el análisis y evaluación del riesgo de información de la empresa.
- Asegura una correcta y segura operación de información de la empresa, reduciendo el riesgo del error humano.
- Incrementa sustancialmente los controles de acceso a la información.
- Minimiza la interrupción en el funcionamiento de las actividades del negocio y lo protege de desastres y fallas mayores.
- Mayor confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.

CAPÍTULO V
DISCUSIÓN Y APLICACIONES

5.1 Análisis de brechas

Como se observa en el capítulo anterior, antes de la implementación, el análisis de brechas PRE dio como resultado tan solo un 34% de cumplimiento de los requisitos de la Circular Nº G-140, teniendo un gran espacio que no estaba siendo atendido.

Después del análisis, gestión y tratamiento del riesgo, proceso en el cual se implementaron todos los controles preventivos, detectivos y correctivos necesarios para minimizar la brecha, se logró mejorar drásticamente el porcentaje de cumplimiento a un 67%.

En este punto del trabajo ya se tiene conocimiento de que un SGSI no es solo tratamiento de los riesgos, para poder minimizar aún más la brecha, se implementó un plan alterno, en el cual se incluyeron muchos ítems para el mantenimiento del sistema de gestión, logrando de esta manera cumplir con un 86% del total de requisitos de la circular Nº G-140.

De aquí en adelante, la empresa se compromete a mejorar continuamente su SGSI y así ir mitigando los riesgos actuales y futuros e ir parchando ciertos puntos para minimizar al máximo la brecha existente.

5.2 Análisis de indicadores

- **Objetivo 1:**

  Al iniciar el proyecto no existía una política de seguridad de información y mucho menos la cultura para proteger los activos de información. Se puede observar una mejoría de 78%.5 en promedio de los dos indicadores. Actualmente los colaboradores de la gerencia de

tecnología conocen como sus funciones cotidianas aportan al mantenimiento y mejora continua del SGSI implementado.

- **Objetivo 2:**

Con los resultados obtenidos después de la implementación del SGSI, se lograron detectar de manera preventiva las vulnerabilidades, mitigando así los futuros riesgos.

De igual manera, se logró implementar procesos de atención inmediata para las vulnerabilidades e incidentes reportados.

- **Objetivo 3:**

Al iniciar el proyecto, se detectó:

- Activos de información sin controles para los cuales se implementaron diferentes tipos de controles preventivos, correctivos y detectivos.
- Muchos riesgos con calificativo no tolerables, los cuales se lograron minimizar a un 0 %.

- **Objetivo 4:**

Si bien todos los colaboradores involucrados en los procesos de tecnología están muy bien entrenados para el cumplimiento de sus labores, no contaban con una formación y concientización sobre la seguridad de información y protección de los activos de información.

Se puede observar que después de la implementación del SGSI, los colaboradores incrementaron notablemente su compromiso con la seguridad de los activos de información.

- **Objetivo 5:**

Después de los análisis de brechas PRE y POST, se observa que el cumplimiento de la circular Nº G-140 mejora en un 52%. Aun así existe una pequeña brecha por cumplir, en la cual la empresa deberá seguir trabajando para cubrirla.

- **Objetivo 6:**

Card Perú S.A. no contaba con la documentación mínima necesaria para soportar un SGSI.

Se puede observar que al final de la implementación se logró contar con toda la documentación necesaria.

5.3 Análisis de los beneficios

- Provee a la gerencia dirección y apoyo para gestionar la seguridad de la información.
- Ayuda a identificar los activos de información y a protegerlos adecuadamente.
- Enfoque sistemático para el análisis y evaluación del riesgo de información de la empresa.
- Asegura una correcta y segura operación de información de la empresa, reduciendo el riesgo del error humano.
- Incrementa, sustancialmente, el control de acceso a la información.
- Minimiza la interrupción en el funcionamiento de las actividades del negocio.
- Demuestra confianza al mercado, proveedores y sociedad.

CONCLUSIONES

1. El implementar una política de seguridad y que los colaboradores la conozcan e interiorizan, es de gran utilidad cuando se quiere implementar cualquier sistema de gestión en una organización, ya que les da una visión clara de cómo sus labores cotidianas aportan para el mantenimiento y mejora de un sistema de gestión empresarial.

2. Aún después de implementar un buen sistema de gestión de seguridad de información, en el futuro se presentan más activos de información, más amenazas, vulnerabilidades y por lo tanto, mayores riesgos. Este escenario no se puede evitar; es por ello que se concluye, que se debe estar preparado para actuar de manera inmediata ante cualquier nueva vulnerabilidad que se identifique.

3. Diseñando e implementando una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afecten a los activos de información.

4. El factor humano es crítico para la implementación de cualquier sistema de gestión organizacional es por ello que la formación y concientización de los mismos es indispensable para lograr una implementación exitosa.

5. Muchas veces las empresas crecen de manera desordenada, crecen con paradigmas equivocados, algunos quieren documentar todo lo que se pueda, otras creen que documentar los procesos es una pérdida de tiempo.

De lo anterior se concluye que la documentación de los procesos es una herramienta poderosa para el mantenimiento y mejora de cualquier sistema de gestión organizacional.

RECOMENDACIONES

1. Se recomienda mantener una constante revisión de la política del SGSI y verificar el cumplimiento de la misma por parte de los empleados de la organización.

2. Se recomienda establecer los mecanismos que permitan la identificación de nuevos activos de información, y también la cultura organizacional para tomar acciones correctivas frente a nuevas vulnerabilidades, amenazas o riesgos detectados; y con base en esa información tomar acciones preventivas

3. Se recomienda seguir con la utilización de una metodología para gestionar los riesgos; ya que, de esta manera se puede lograr una reducción en los riesgos a los cuales son sometidos los activos de información y también se puede hacer lo mismo para nuevos riesgos que aparezcan.

4. Se recomienda formar y capacitar de manera periódica al personal en temas de seguridad de la información y así lograr que todos los involucrados o relacionados con los activos de información tengan los alcances de la implementación claros.

5. Se recomienda la revisión periódica de la circular G-140 para verificar si existen cambios en los requisitos legales que impacten en el SGSI.

6. Se recomienda realizar una documentación de procesos para poder gestionar los mismos de manera óptima y hacer frente a cualquier cambio

que se pueda dar en la organización. La documentación de procesos también nos permite la mejora de estos.

FUENTES DE INFORMACIÓN

Fuentes bibliográficas

1. Alexander, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información. Primera edición. Colombia: Alfaomega, 2007.
2. International Organization of Standardization and International ElectrotechnicalCommission. ISO/IEC 27001:2005 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Primera edición, 2005.
3. International Organization of Standardization and International Electrotechnical Commission. ISO/IEC 17799:2005. Tecnologías de la Información – Técnicas de Seguridad – Código para la práctica de la gestión de la seguridad de la información. Segunda Edición, 2005.
4. International Organization of Standardization and International Electrotechnical Commission. ISO/IEC 27004:2009 Tecnología de la Información – Técnicas de seguridad – Gestión de la seguridad de la información – Medición, 2009.
5. Project Management Institute. Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK). Cuarta edición, 2008.
6. Ley N° 26702 “Texto Concordado de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, 1996.

Fuentes electrónicas

1. Bsigroup. ¿Qué son los sistemas de gestión?, 2012. Disponible en: http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/De-un-vistazo/Que-son-los-sistemas-de-gestion/. Consultado Diciembre 02, 2011.
2. Vergara, Gonzalo. (2009)¿Qué es un sistema de gestión? Disponible en: http://mejoratugestion.com/mejora-tu-gestion/que-es-un-sistema-de-gestion/. Consultado Diciembre 02, 2011.
3. Wikipedia. (2011). Seguridad de la información. Disponible en: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n. Consultado Diciembre 3, 2011.
4. mmc.geoFÍSICA.unam.mx. (2003). Políticas de seguridad. Disponible en: http://mmc.geoFÍSICA.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node333.html. Consultado Diciembre 5, 2011.
5. Basc-costarica. Fecha desconocida. (4 páginas). Política de Seguridad. Disponible en: http://www.basc-costarica.com/documentos/politica-seguridad.pdf. Consultado Diciembre 5, 2011.
6. Chapin, David A. y Akridge, Steven. (2005)¿Cómo Puede Medirse la Seguridad? Disponible en: http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf. Consultado Diciembre 9, 2011.
7. Diario Gestión. (2010). Tarjetas de crédito acelerarían crecimiento en último trimestre. Disponible en: http://gestion.pe/noticia/667537/tarjetas-credito-acelerarian-crecimiento-ultimo-trimestre. Consultado Diciembre 10, 2011.
8. Stakeholders. (Fechas desconocida). Telefónica obtiene certificación ISO 27001. Disponible en: http://www.stakeholders.com.pe/index.php?option=com_content&task=view&id=2097. Consultado Diciembre 11, 2011.

9. Diario El Economista. (2006). Bankinter recibe la certificación internacional ISO 27001 para sus sistemas de seguridad informática. Disponible en: http://www.eleconomista.es/empresas-finanzas/noticias/108827/11/06/Bankinter-recibe-la-certificacion-internacional-ISO-27001-para-sus-sistemas-de-seguridad-informatica.html. Consultado Diciembre 11, 2011.
10. Iso27001certificates. Disponible en: http://www.iso27001certificates.com. Consultado Diciembre 12, 2011.
11. Consumoteca. (2009). Entidad financiera. Disponible en: http://www.consumoteca.com/diccionario/entidad-financiera. Consultado Diciembre 12, 2011.
12. Archivólogo. (2011). PERDIDAS FINANCIERAS POR FUGA DE INFORMACIÓN. Disponible en: http://archivologo.blogcindario.com/2011/02/02874-perdidas-financieras-por-fugas-de-información.html. Consultado Diciembre 15, 2011.

ANEXOS

Anexo 01: circular n° g-140

Lima, 02 de abril de 2009

CIRCULAR Nº G-140-2009

Ref.: Gestión de la seguridad de la información

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias en adelante Ley General, y por el inciso d) del artículo 57° del Texto Unico Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones, las cuales toman como referencia estándares internacionales como el ISO 17799 e ISO 27001, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

Alcance
Artículo 1º.- La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Definiciones
Artículo 2º.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

b. Factor de autenticación: Información utilizada para verificar la identidad de una persona. Pueden clasificarse de la siguiente manera:
   - Algo que el usuario conoce (por ejemplo: una clave de identificación)
   - Algo que el usuario posee (por ejemplo: una tarjeta)
   - Algo que el usuario es (por ejemplo: características biométricas)

c. Incidente de seguridad de información: Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

d. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

e. Ley General: Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias.

f. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:

   I. Confidencialidad: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
   II. Integridad: La información debe ser completa, exacta y válida.
   III. Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

g. Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.

h. Subcontratación significativa: Aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, o continuidad operativa.

Sistema de gestión de la seguridad de la información

Artículo 3°.- Las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI).

Las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

a. Definición de una política de seguridad de información aprobada por el Directorio.
b. Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
c. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Estructura organizacional

Artículo 4°.- Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información señalado en el artículo anterior.

Asimismo, deben asegurarse que se desarrollen las siguientes funciones, ya sea a través de una unidad especializada o a través de alguna de las áreas de la empresa:

a. Asegurar el cumplimiento de la política de seguridad de información y de la metodología definida por la empresa.
b. Coordinar y monitorear la implementación de los controles de seguridad de información.
c. Desarrollar actividades de concientización y entrenamiento en seguridad de información.
d. Evaluar los incidentes de seguridad de información y recomendar acciones apropiadas.

La Superintendencia podrá requerir la creación de una unidad especializada en gestión de la seguridad de información en empresas que a su criterio resulten complejas, y cuando se observe en el ejercicio de las acciones de supervisión que no se cumple con los criterios previstos en la normativa vigente.

Controles de seguridad de información

Artículo 5°.- Como parte de su sistema de gestión de la seguridad de información, las empresas deberán considerar, como mínimo, la implementación de los controles generales que se indican en el presente artículo.

5.1 Seguridad lógica

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.
b) Revisiones periódicas sobre los derechos concedidos a los usuarios.
c) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
d) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
e) Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.
f) Controles especiales sobre usuarios remotos y computación móvil.

5.2 Seguridad de personal

a) Definición de roles y responsabilidades establecidos sobre la seguridad de información.
b) Verificación de antecedentes, de conformidad con la legislación laboral vigente.
c) Concientización y entrenamiento.
d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.
e) Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.

5.3 Seguridad física y ambiental

a) Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.
b) Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.

5.4 Inventario de activos y clasificación de la información

a) Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.
b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

5.5. Administración de las operaciones y comunicaciones

a) Procedimientos documentados para la operación de los sistemas.
b) Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
c) Separación de funciones para reducir el riesgo de error o fraude.
d) Separación de los ambientes de desarrollo, pruebas y producción.
e) Monitoreo del servicio dado por terceras partes.
f) Administración de la capacidad de procesamiento.
g) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
h) Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
i) Seguridad sobre el intercambio de la información, incluido el correo electrónico.
j) Seguridad sobre canales electrónicos.
k) Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.

5.6. Adquisición, desarrollo y mantenimiento de sistemas informáticos

Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
d) Controlar el acceso a las librerías de programas fuente.
e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.
f) Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.

5.7. Procedimientos de respaldo

a) Procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la empresa.

b) Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento.

5.8. Gestión de incidentes de seguridad de información

Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, las empresas deberán considerar los siguientes aspectos:

a) Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.
b) Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

5.9. Cumplimiento normativo

Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

5.10. Privacidad de la información

Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.

Seguridad en operaciones de transferencia de fondos por canales electrónicos

Artículo 6°.- En el caso de las operaciones de transferencia de fondos a terceros ofrecidas por las empresas para su realización a través de canales electrónicos, las empresas deberán implementar un esquema de autenticación de los clientes basado en dos factores como mínimo. Para el caso en que el canal electrónico sea Internet, uno de los factores de autenticación deberá ser de generación o asignación dinámica. Las empresas podrán utilizar otros factores de autenticación, en tanto éstos proporcionen un nivel de seguridad equivalente o superior respecto a los dos factores señalados, en particular cuando se trate de operaciones importantes según los límites que el banco determine de acuerdo a las características del producto o servicio ofrecido.

La empresa deberá tomar en cuenta los riesgos operacionales asociados, en el diseño de los procedimientos, las definiciones de límites y las consideraciones de seguridad e infraestructura requeridas para un funcionamiento seguro y apropiado en las operaciones de transferencia de fondos.

Subcontratación

Artículo 7°.- Las empresas son responsables y deben verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en el artículo 21° del Reglamento de la Gestión Integral de Riesgos. Asimismo, las empresas deben asegurarse que el procesamiento y la información objeto de la subcontratación, se encuentre efectivamente aislada en todo momento.

En caso que las empresas deseen realizar una subcontratación significativa de su procesamiento de datos, de tal manera que éste sea realizado en el exterior, requerirán de la autorización previa y expresa de la Superintendencia. Para ello, la empresa debe asegurar un adecuado cumplimiento de la presente Circular, en lo que sea aplicable al servicio de procesamiento contratado.

La Superintendencia podrá requerir cuando así lo considere apropiado que el proveedor del servicio en el exterior se encuentre sujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio.

En el Anexo A que forma parte de la presente norma y se publica en el Portal electrónico institucional (**www.sbs.gob.pe**), conforme a lo dispuesto en el Decreto Supremo N° 001-2009-JUS, se detalla la información que debe remitir la empresa adjunta a su solicitud de autorización. Una vez recibida la documentación completa, dentro de un plazo que no excederá de sesenta (60) días útiles, la Superintendencia emitirá la resolución que autoriza o el oficio que deniega la solicitud presentada por la empresa.

Las empresas que obtengan la autorización para realizar su procesamiento de datos en el exterior, deberán asegurar, con una frecuencia anual, que el servicio subcontratado sea sometido a un examen de auditoría independiente, por una empresa auditora de prestigio, que guarde conformidad con el estándar SAS 70 emitido por el Instituto Americano de Contadores Públicos Certificados (AICPA). En tal sentido, las empresas deberán remitir a la Superintendencia el Reporte de Auditoría de Tipo II considerado en dicho estándar, el cual entre otros aspectos considera la evaluación de los controles implementados y las pruebas de su efectividad.

Información a la Superintendencia
Artículo 8°.- Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la gestión del riesgo operacional, emitido por la SBS, las empresas deberán incluir información sobre la gestión de la seguridad de la información.

Información adicional
Artículo 9°.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión de la seguridad de la información de la empresa.

Asimismo, la empresa deberá tener a disposición de la Superintendencia todos los documentos a que hace mención la presente Circular, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de ser aplicable.

Sanciones
Artículo 10°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Vigencia
Artículo 11°.- Las disposiciones de la presente Circular entran en vigencia al día siguiente de su publicación en el Diario Oficial "El Peruano", otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010, fecha a partir de la cual quedará sin efecto la Circular SBS N° G-105-2002.

Adecuación de las AFP
Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las AFP deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico de la situación existente en la AFP respecto al cumplimiento de cada uno de los artículos de la presente Circular, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Atentamente,

FELIPE TAM FOX
Superintendente de Banca, Seguros y

ANEXO A

DOCUMENTACIÓN A REMITIR JUNTO CON LA SOLICITUD DE AUTORIZACIÓN PARA REALIZAR PROCESAMIENTO PRINCIPAL EN EL EXTERIOR

Documento	Contenido mínimo requerido
1. Información general del proveedor y del servicio	• Razón social del proveedor. • Giro del negocio y años de experiencia. Indicar a qué empresas brinda servicios actualmente. • Estados Financieros del proveedor correspondientes a los dos últimos años. • Relación de accionistas del proveedor y funcionarios principales. • Relación con la empresa supervisada (indicar si pertenecen al mismo grupo económico). • Servicios que serán provistos por el proveedor y el tipo de información a ser procesada. • Ubicación (país y ciudad) del centro de procesamiento principal. • Razones para seleccionar al proveedor.
2. Borrador del Contrato	Aspectos a considerar: • Acuerdos de niveles de servicio. • Procedimientos de monitoreo. • Procedimientos de contingencia. • Cumplimiento de las normas sobre secreto bancario y confidencialidad de la información. • Prestación del servicio en regímenes especiales (vigilancia, intervención, liquidación). El proveedor debe seguir brindando el servicio como mínimo un año después de que la empresa ha ingresado a un régimen especial. • Compromiso de cumplimiento de la normativa de la Superintendencia. • Aseguramiento del acceso adecuado a la información con fines de supervisión, en tiempos razonables y a solo requerimiento, por parte de la Superintendencia, Auditoría Interna y Externa, en condiciones normales de operación y en regímenes especiales. Este aspecto debe ser aplicable sobre cualquier otra empresa que el proveedor subcontrate para brindar servicios a la entidad supervisada. • Cláusulas que faciliten una adecuada revisión por parte de la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa y la Superintendencia.
3. Informe de la Plataforma Tecnológica	Aspectos a considerar: (Señalar qué equipos y aplicaciones estarán a cargo del proveedor) • Inventario de equipos de cómputo. • Inventario de software base. • Herramientas y/o manejadores de base de datos. • Aplicaciones críticas. • Esquema de comunicaciones a ser implementado entre el proveedor y la empresa supervisada.
4. Informe de Comunicación con la	• Descripción de la forma de envío de información a la Superintendencia luego de que se implemente el servicio de procesamiento en el exterior. Asimismo, indicar los cambios que se aplicarán sobre los procedimientos asociados a la

	Superintendencia (SUCAVE, RCD, otros)	generación, consolidación y reporte de dicha información.
5.	Informe de Evaluación de Riesgos	• Evaluación de los riesgos de operación asociados con el esquema propuesto por la empresa, realizada por la Unidad de Riesgos.
6.	Gestión de la seguridad de información	• Política de seguridad de información de la empresa. • Estructura organizativa para la gestión de la seguridad de información. • Asignación de responsabilidades asociadas con la seguridad de información en la entidad y el proveedor. • Forma en que se aislará el procesamiento y la información objeto de la subcontratación. • Procedimientos y controles a implementar, considerando el procesamiento en el exterior, en los siguientes aspectos: - Seguridad lógica. - Seguridad de personal. - Seguridad física y ambiental. - Administración de las operaciones y comunicaciones. - Desarrollo y mantenimiento de los sistemas informáticos. - Administración de las copias de respaldo.
7.	Gestión de continuidad de negocios	• Plan de Contingencia del proveedor, para asegurar la continuidad del servicio de procesamiento informático. • Señalar la prioridad asignada al procesamiento de la información de la empresa supervisada respecto al resto de clientes del proveedor. • Señalar la forma en que se dará aviso a la empresa supervisada, y las acciones que deberá desarrollar la empresa en caso de una contingencia en el proveedor. • Frecuencia y alcance de las pruebas al Plan de Contingencia del proveedor.
8.	Plan de Auditoría de Sistemas	• Señalar el alcance, forma y periodicidad de las revisiones de auditoría de sistemas considerando el nuevo esquema de procesamiento principal de la empresa.
9.	Gestión del proyecto	• Cronograma de actividades, incluyendo plazos, responsables y principales hitos de control. • Costo estimado de implementación del proyecto.

Anexo 02: marco lógico

Análisis de involucrados

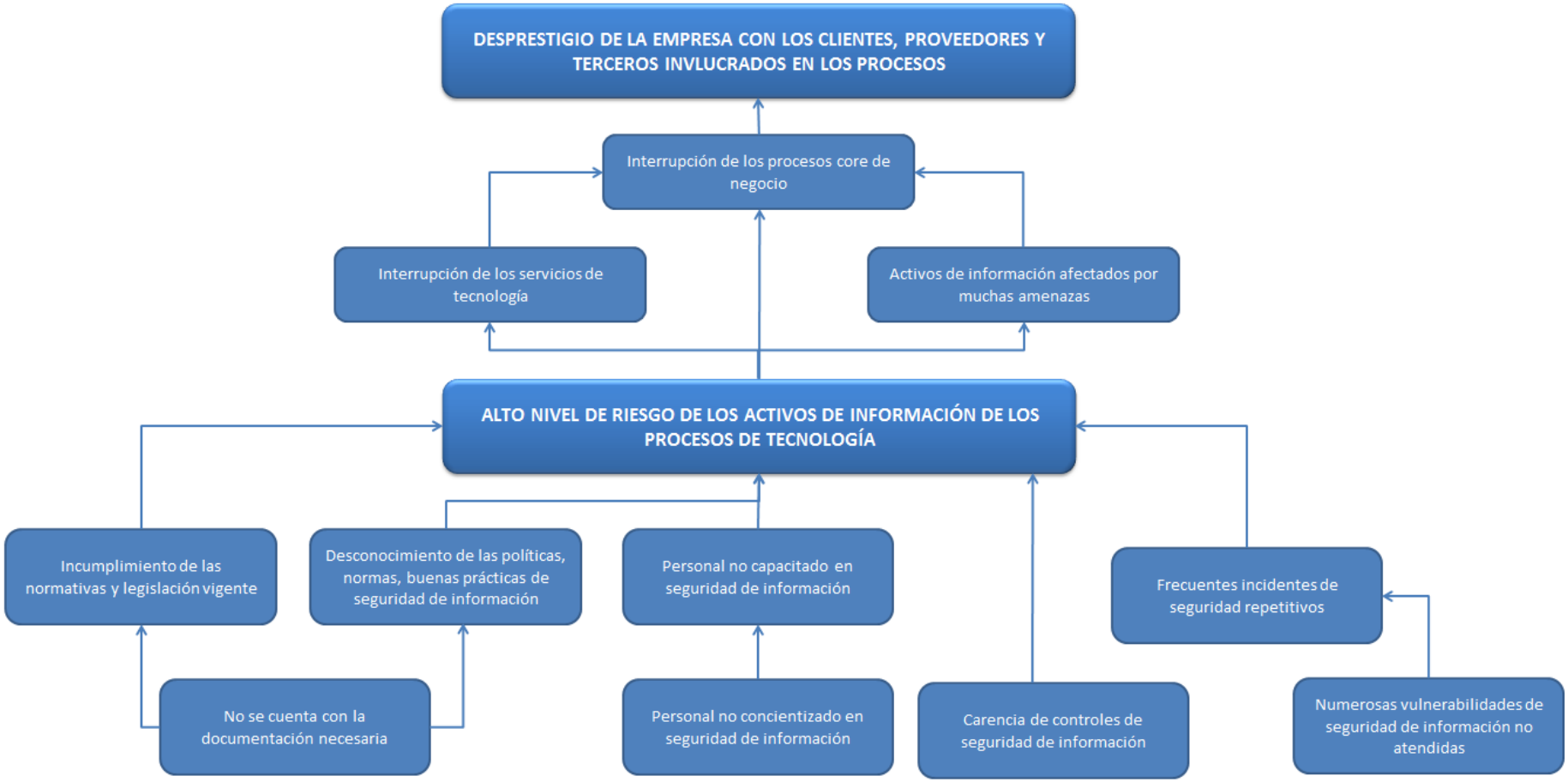
CUADRO DE INVOLUCRADOS			
Grupos	**Problemas Percibidos**	**Intereses**	**Recursos/Mandatos**
Áreas de Tecnología	* Frecuentes incidentes de seguridad repetitivos	* Minimizar los incidentes de seguridad repetitivos	**R:** Personal calificado multidisciplinario para la solución de los problemas identificados. **R:** Falta de recursos tecnológicos necesarios **M:** Disponibilidad financiera para adquirir lo necesario. **M:** Alto compromiso de la gerencia de tecnología para mitigar lo problemas percibidos.
	* Números vulnerabilidades asociadas a la seguridad de información no atendidas	* Eliminar las vulnerabilidades asociadas a la seguridad de información	
	* Altos niveles de riesgo de los activos de información	* Mitigar los riesgos de los activos de información	
	* Personal no capacitado en seguridad de información	* Contar con el todo el personal capacitado en seguridad de la información	
	* Personal no concientizado en seguridad de información	* Contar con todo el personal concientizado en seguridad de la información	
	* No se cuenta con la documentación necesaria	* Contar con la documentación requerida y necesaria	
Alta Gerencia	* Incumplimiento de normativas y legislación vigentes	* Cumplir con las normas y legislaciones vigentes de una financiera	**M:** Poder para hacer cumplir las normas, legislaciones y requisitos normativos.
Áreas usuarias (Clientes internos)	* Interrupción de los servicios de tecnología	* Continuidad de los servicios de tecnología	**M:** Bajo conocimiento de los usuarios para detectar fallo de servicios **R:** No se cuenta con recursos para reportar caída de servicios.
Clientes externos	* Interrupción de los servicios de giro de negocio	* Continuidad de los servicios de giro de negocio de cada al cliente	**M:** Poder para cancelar los procesos de la empresa.

Proveedores	* Desconocimiento de las políticas, normas, buenas prácticas de seguridad de información	* Contar con políticas, normas y buenas prácticas desplegadas con los colaboradores, clientes, proveedores y otras partes interesadas	**M:** Disponibilidad para cumplir con las políticas, buenas prácticas, procedimientos que la empresa establezca. **R:** Recursos tecnológicos para mitigar la interrupción de los servicios brindados.
	* Interrupción de los servicios de tecnología	* Continuidad de los servicios de tecnología	

Cuadro: Análisis de involucrados [69]

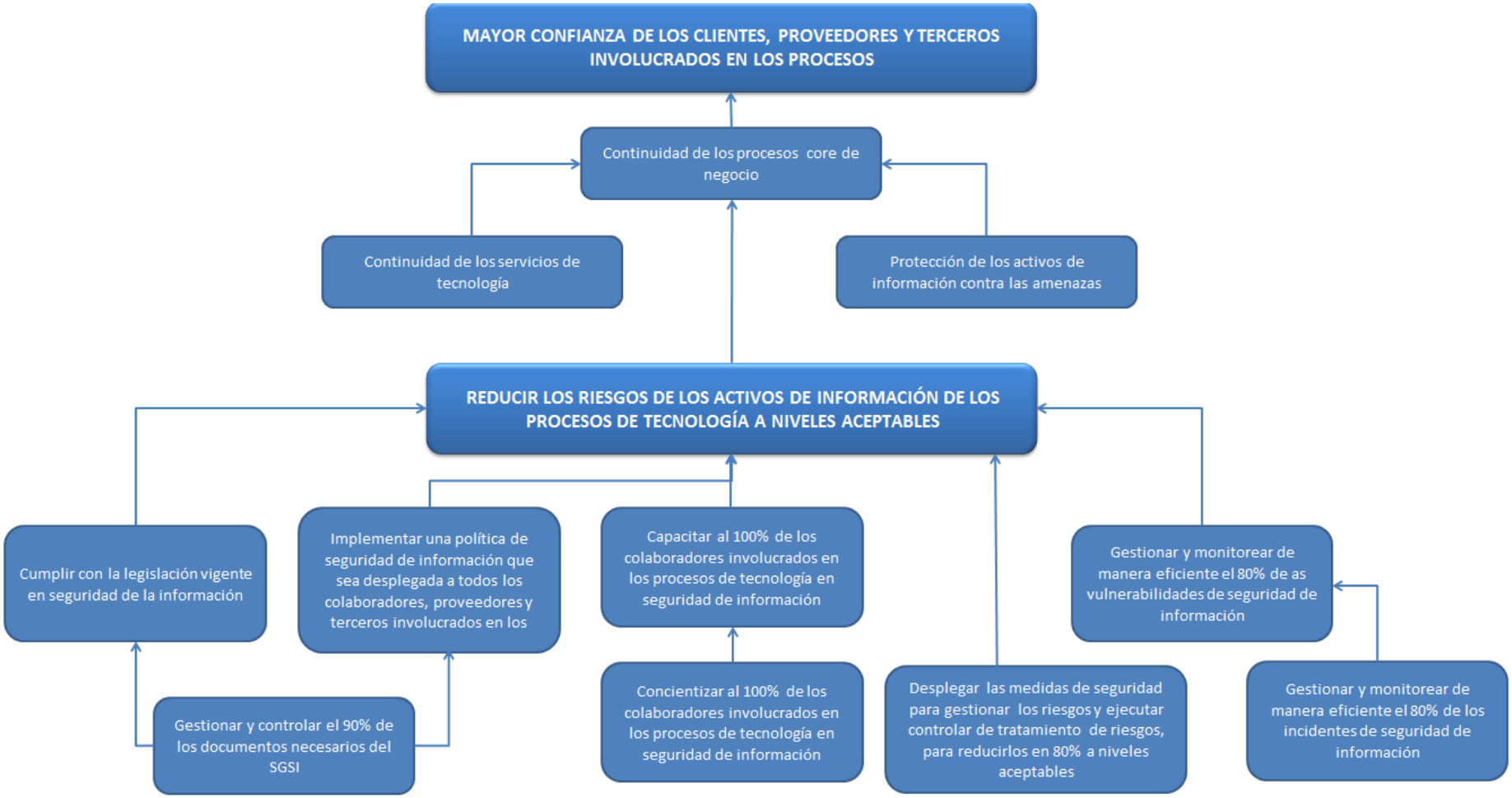
[69] Elaboración: los autores.

Árbol de problemas [70]



[70] Fuente: Gráfico elaborado por el grupo de proyecto en el cual se muestra el árbol de problemas del proyecto.

Árbol de objetivos [71]



[71] Fuente: Gráfico elaborado por el grupo de proyecto en el cual se muestra el árbol de objetivos del proyecto.

Matriz de marco lógico

Resumen Narrativo	Indicadores (%)	Medios de Verificación	Supuestos
Fin:			
Asegurar la continuidad y normalidad de los procesos y servicios de tecnología.	Procesos afectados por la materialización de una amenaza de seguridad de información	- Reportes de procesos	Todos los eventos anormales son registrados
Propósito:			
Mitigar y reducir los riesgos de los activos de información de los procesos de tecnología a niveles aceptables.	Cumplimiento el proyecto en los plazos definidos	- Seguimiento mensual de cumplimiento del proyecto. - Control de cambios - Gestión de riesgos del proyecto	Colaboradores comprometidos, concientizados y capacitados para la implementación
Componentes:			
Implementar una Política de Seguridad de Información que sea desplegada a todos los colaboradores, proveedores y terceros involucrados en los procesos de Tecnología	Colaboradores que conocen la política de seguridad de Información	Entrevistas y encuestas	Cumplimiento de la política SGSI
	Colaboradores consientes de la política de seguridad de Información		
	Colaboradores que cumplen de la política de seguridad de Información	Evidencias visuales	
Gestionar y monitorear de manera eficiente las vulnerabilidades e incidentes de seguridad de información.	Incidentes reportados adecuadamente	Registro de incidentes reportados	Todos los incidentes reportados son registrados
	Vulnerabilidades reportadas adecuadamente	Registro de vulnerabilidades reportadas	Todas las vulnerabilidades reportadas son registradas
	Incidentes atendidos oportunamente	Reporte de incidentes atendidos	Todos los incidentes atendidos son registrados
	Vulnerabilidades atendidos oportunamente	Reporte de vulnerabilidades atendidas	Todas las vulnerabilidades atendidos son registradas

Desplegar medidas de seguridad para mitigar los riesgos.	Activos de información sin mecanismos de control	Matriz de identificación de riesgos	Tratamiento de todos los riesgos inaceptables
	Activos de información con más de tres vulnerabilidades		Identificación de vulnerabilidades actualizadas
	Riesgos con nivel de tolerancia “no tolerables”		Cálculo del riesgo según la metodología
	Riesgos con nivel de tolerancia “totalmente tolerables”		Calculo del riesgo según la metodología
Formación y concientización de los colaboradores involucrados en los procesos de tecnología en temas de seguridad.	Colaboradores capacitados/concientizados	Lista de asistencia a capacitaciones	Capacitación a todo el personal involucrado
	Colaborares capacitados/concientizados aprobados > 15	Resultado de evaluaciones	Prueba de evaluación con complejidad media
Cumplimiento de legislación vigente de seguridad.	Cumplimiento de requisitos reglamentarios	Resultado de análisis GAP.	Todos los requisitos legales son basados en la circular N° G.140
Gestionar y controlar el 100% de los documentos del SGSI.	Procedimientos necesarios SGSI documentados/ estandarizados/ difundidos (DED)	Lista maestra de documentos de seguridad.	Todos los documentos necesarios son basados en la circular N° G-140
	Cumplimiento de los procedimientos SGSI documentados/ estandarizados/ difundidos (DED)	Entrevistas con involucrados, jefaturas y gerencias (auditoria de cumplimiento)	
Actividades:			
- Actividades para la gestión y seguimiento del proyecto de diseño e implementación	Cumplimiento de las actividades en los plazos definidos	- Informe de avances del proyecto	- Participación completa de los involucrados
- Análisis de brechas PRE			
- Elaborar la política de SGSI			

- Reporte y tratamiento de incidentes y vulnerabilidades			
- Análisis y evaluación de riesgos			
- Elaborar el plan de tratamiento de riesgos			
- Implementar los planes de tratamiento de riesgos para todos los procesos de tecnología			
- Elaborar las pruebas y resultados de implementación			
- Capacitación y concientización de los colaboradores			
- Implementar el sistema documentario SGSI			
- Presentación final y aprobación de proyecto			

Cuadro: Matriz de marco lógico [72]

[72] Elaboración: los autores.

Análisis de alternativas

El siguiente cuadro muestra el análisis de alternativas realizado, en el cual se considera una implementación de una metodología de gestión de riesgos general, una implementación de un SGSI enfocado a la circular N° G-140 o una certificación de un SGSI enfocado a la ISO 27001. Para el análisis se consideró una comparación cualitativa y otra cuantitativa.

En el cuadro de escala de criterios, se observa dos valores (valor 1 y valor 2). El valor 1 incluye los criterios que son evaluados de forma positiva, como son: competitividad, viabilidad, prioridad, regulatorio. El valor 2 incluye los criterios que son evaluados de forma negativa como son: costo, riesgos, tiempo, complejidad.

Escala de Criterios	Valor 1	Valor 2
Muy Bajo	10	50
Bajo	20	40
Medio	30	30
Alto	40	20
Muy Alto	50	10

De acuerdo con la evaluación mostrada, la alternativa elegida es la alternativa 2: implementación de un SGSI enfocado a la circular N° G-140, debido a que tiene un mayor valor ponderado (38.5) respecto a aspectos considerados.

Comparación Cualitativa		Alternativas		
		Alternativa 1: Implementación de Metodologías de Gestión de Riesgos	**Alternativa 2: Implementación de un SGSI enfocado a la Circular N° G-140**	Alternativa 3: Certificación de un SGSI enfocado a la ISO 27001
c	Costo	Bajo	Alto	Muy alto
r	Riesgos	Bajo	Bajo	Medio
i	Tiempo	Muy Bajo	Bajo	Alto
t	Complejidad	Bajo	Medio	Muy Alto
e	Competitividad	Muy Bajo	Alto	Muy Alto
r	Viabilidad	Muy Alto	Muy Alto	Alto
i	Prioridad	Alto	Muy Alto	Bajo
o	Regulatorio	Bajo	Muy Alto	Bajo

Comparación Cualitativa			Alternativas		
			Alternativa 1: Implementación de Metodologías de Gestión de Riesgos	**Alternativa 2: Implementación de un SGSI enfocado a la Circular N° G-140**	Alternativa 3: Certificación de un SGSI enfocado a la ISO 27001
c	Costo	20%	40	20	10
r	Riesgos	10%	40	40	30
i	Tiempo	18%	50	40	20
t	Complejidad	5%	50	20	10
e	Competitividad	12%	10	40	50
r	Viabilidad	10%	50	50	40
i	Prioridad	10%	40	50	20
o	Regulatorio	15%	20	50	20
		100%	**36.7**	**38.5**	**24.1**

Cuadro: Análisis de alternativas [73]

[73] Fuente Elaboración de los autores.

Anexo 03: comparación de metodologías

El siguiente cuadro muestra comparación de metodologías realizadas, en las cuales se considera una implementación de una metodología de gestión de riesgos utilizando las mejores prácticas de la metodología 1 y 2. Para el análisis se consideró una comparación cuantitativa.

Escala de Criterios	Valor 1
Muy Bajo	10
Bajo	20
Medio	30
Alto	40
Muy Alto	50

En este caso, la metodología 3: Híbrido propuesto (metodología creada por el equipo de proyecto utilizando las mejores prácticas de las anteriores y haciendo mejoras) debido a que tiene una mejor ponderación (42) respecto a las otras metodologías propuestas.

			Alternativas para la Gestión y Control de Riesgos de Activos de Información		
			Metodología 1*: Magerit	Metodología 2*: Metodología de gestión de riesgos (Alexander, 2007)	**Metodología 3: Híbrido Propuesto**
Criterios	Costo	10%	40	40	40
	Riesgos del Proyecto	10%	40	30	40
	Tiempo	25%	20	30	40
	Complejidad	20%	20	30	40
	Uso de recursos	15%	40	40	40
	Flexibilidad	20%	20	20	50
		100%	**27**	**30.5**	**42**

Cuadro: Comparación de metodologías [74]

[74] Elaboración: los autores.

Anexo 04: buenas prácticas ambientales [75]

Buenas prácticas ambientales durante la implementación del SGSI

Con este documento para las buenas prácticas ambientales, se busca minimizar el impacto ambiental que ocasionará el implementar un SGSI documentado, para ello se deben cumplir las siguientes buenas prácticas:

- ✓ Poner el ordenador en sistema de ahorro de consumo, configurar el salvapantallas en modo “pantalla en negro”, ya que ahorra energía. Es aconsejable un tiempo de 10 minutos para que entre en funcionamiento este modo.
- ✓ Si su ordenador dispone de opciones “EnergyStar” o “ahorro de energía” asegúrese de que están activadas; los equipos a menudo tienen estas opciones desactivadas cuando son configurados.
- ✓ Los protectores de pantalla no ahorran energía. Active las opciones de desconexión e insista al personal para que desconecten al menos los monitores de sus ordenadores (utilizan dos veces la energía de un PC) cuando no se esté utilizando, así como cuando abandonan sus mesas para asistir a reuniones o para el almuerzo.
- ✓ Asegurarse de que el ordenador (incluida la pantalla) queda apagado al final de la jornada de trabajo.
- ✓ Apagar las luces del puesto de trabajo cuando no sean necesarias.
- ✓ Uso de cartuchos reciclados.
- ✓ Agitar el cartucho de tóner cuando la impresora da el aviso de que está bajo (puede dar para 100 copias más).
- ✓ Devolver los cartuchos de tóner usados para su reciclaje a través de una empresa especializada en su reciclado.
- ✓ Uso de papel reciclado para la impresión de documentos.
- ✓ Escribir, imprimir y fotocopiar por las dos caras, siempre que sea posible.
- ✓ Usar el papel escrito por una cara como papel borrador para documentos de revisión.

[75] Fuente: Se muestra información sobre buenas prácticas ambientales, la cual fue extraída del siguiente enlace:
http://www.camarazaragoza.com/medioambiente/docs/buenaspracticas/buenaspracticas3.pdf