Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Propuesta de Trabajo Final

Tema

Gestión Estratégica de Seguridad Informática

Título

MODELIZACIÓN DE UN PROCESO DE CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN MEDIANTE LA IMPLEMENTACIÓN DE UNA SOLUCIÓN INFORMÁTICA PARA UNA ENTIDAD FINANCIERA

Autor/a: Mariela Diannet Condori Rivera

Tutor/a del Trabajo Final

Mg. Marcia L. Maggiore

Año de Presentación

2017

Cohorte del Cursante

2013

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual

Mariela Condori Rivera

DNI 95128741

Resumen

En la actualidad las organizaciones necesitan apoyarse en la tecnología para maximizar la eficiencia y eficacia de sus procesos, y así poder obtener resultados en el menor tiempo posible para la toma de decisiones de la alta gerencia(1).

La automatización de procesos en las diferentes áreas de una organización genera un valor agregado en el cumplimiento de sus objetivos así como también en la exactitud de los datos generados en los reportes y en una mejora considerable del tiempo de trabajo del personal involucrado en el proceso(2).

En este trabajo se presentará un enfoque del diseño y la implementación de un proceso automatizado para la "Clasificación de activos", utilizando una herramienta informática GRC[1]aplicada en una entidad financiera.

A lo largo del desarrollo del trabajo, se expondrá la metodología para el diseño e implementación de clasificación de activos.

Se mostrará las ventajas comparativas entre el proceso automatizado de clasificación de activos y el proceso de clasificación de activos de modo convencional, demostrándose de esta manera el valor agregado que genera la automatización del proceso de clasificación de activos.

Palabras Clave: activos, clasificación de activos, herramienta informática GRC(Gobierno, riesgo y cumplimiento).

[1]La herramienta informática utilizada en este trabajo es la Solución Tecnológica RSA Archer eGRC

Tabla de contenido

Tabla de Figuras

Introducción

La clasificación de los activos de información es necesaria para optimizar el manejo de la información. Si se implementa correctamente la clasificación de activos, se podrá reducir los costos protegiendo la información. (3)

La clasificación de la información prioriza el uso de los controles para que los mismos estén aplicados en la información que sea más sensible y no sean aplicados donde no se necesiten. (3)

Los esquemas de seguridad de clasificación mejoran la usabilidad de los datos asegurando la confidencialidad, integridad y disponibilidad de la información. (3)

El proceso de clasificación de activos, que actualmente realizan algunas entidades financieras, utiliza herramientas manuales compuestas por hojas de cálculo y correos electrónicos. Estas herramientas convencionales impiden realizar una adecuada gestión de riesgos, generando mayores costos, ya que posibilitan la duplicidad de la información, el control deficiente en el acceso y la modificación de la información por parte de terceras personas, dificultando así el manejo de la información, impidiendo la generación de reportes oportunos, todo lo cual genera finalmente, el uso ineficiente de los recursos de la organización.

Además se debe considerar las exigencias descritas en la normativa A4609 sección 3. ”Protección de activos de información”, emitida por el Banco Central de la República Argentina (BCRA) que es el ente regulador. Las entidades financieras deben clasificar sus activos de información de acuerdo a su criticidad y sensibilidad, estableciendo adecuados derechos de acceso a los datos administrados en sus sistemas de información. Los niveles de acceso deben diseñarse considerando los criterios de clasificación, junto con una adecuada separación de tareas, determinando qué clase de usuarios o grupos poseen derechos de acceso y con qué privilegios sobre lo datos, sistemas, funciones y servicios informáticos. (4)

Considerando las áreas involucradas en el proceso de clasificación de los activos de información, se determina que los silos de información que maneja cada área dentro de una organización, generan ineficiencias y problemas de comunicación internos, impactando en el rendimiento y la toma de decisiones, por ende dificultan gestionar el negocio. Por tanto es recomendable manejar una sola fuente de información para toda la organización. (5)

Es posible optimizar el proceso de clasificación de activos convencional, utilizando una herramienta informática GRC[2] (las siglas responden a "Gobierno, Riesgo y Cumplimiento"). Esta solución tiene como finalidad automatizar todo el proceso de clasificación de activos, para lograr mayor efectividad y eficiencia en la gestión de riesgos, así como controlar el acceso a la información, ya que permite configurar perfiles y privilegios según los roles de los trabajadores. Además utiliza un único repositorio de información, lo cual evita su duplicación, mejora la visibilidad y permite la generación sencilla de reportes en tiempo real, que posibilitan una adecuada toma de decisiones de la gerencia encargada del activo en riesgo.

En este trabajo se presentará el diseño y la implementación de un proceso informatizado de clasificación de activos para una entidad financiera permitiendo:

- El uso efectivo de una herramienta de información para la gestión GRC
- La definición de un proceso de "clasificación de Activos" junto con sus etapas e integrado en la herramienta informática GRC
- La adaptación del proceso de clasificación de activos a la herramienta GRC

[2]La herramienta informática utilizada en este trabajo es la Solución Tecnológica RSA Archer eGRC

- La generación de reportes de resultados para las diferentes áreas de la entidad

Capítulo 1 - Conceptos Generales

Marco teórico

A continuación, se describen los componentes del proceso de clasificación de los activo de información.

Según ISO/IEC 27002:2013 en el punto 8.2, la clasificación de activos garantiza que la información reciba un apropiado nivel de protección.

¿Qué es un activo?

Elemento que contiene o manipula información que tiene algún valor para la organización y por tanto debe protegerse.

Según la norma ISO/IEC 27002:2013 en el punto 8.1.2 se recomienda que toda la información y activos asociados con las instalaciones de procesamiento de información sean de propiedad de un responsable designado por la organización.

Propietario o Dueño del activo:

Es la persona responsable del activo, aunque no necesariamente sea quién lo gestione cada día.

¿Qué es la clasificación de activos?

Clasificar un activo es estimar qué valor o importancia tienen para la organización.

La clasificación de activos puede ser de dos tipos:

Cuantitativa: Valor económico

Cualitativa: Alto/Medio/Bajo

Para los fines de este trabajo se utilizará la clasificación de activos de tipo cualitativa.

Según la norma ISO/IEC 27002:2013 en el punto 8.2.1. Directrices para la clasificación, "*Es conveniente que la información se encuentre clasificada en términos de su valor, requerimientos legales, sensibilidad y la criticidad para la organización.*".

Pilares de la seguridad de la información

Según la norma ISO 27001son los siguientes:

Confidencialidad: Es la garantía de acceso de la información de los usuarios que se encuentran autorizados para tal fin.

Integridad: Es la preservación de la información completa y exacta.

Disponibilidad: Es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

Proceso de Negocio

Es un conjunto de actividades que son realizadas coordinadamente en el entorno organizacional y técnico.

- Estas actividades, en su conjunto, ayudan a alcanzar un determinado objetivo de negocio.
- Cada proceso de negocio es realizado por una única organización, pero puede interactuar con procesos de otras organizaciones. (6)

BIA (Análisis de impacto en el negocio)

Refleja las etapas iníciales de la planificación de la continuidad del negocio, que consiste en la identificación de riesgos y determinación de los objetivos de tiempo de recuperación (RTO) en orden para establecer los umbrales de riesgo y recuperación de Continuidad del negocio y planes de recuperación de desastres de TI.

¿Por qué Gobierno, Riesgo y Cumplimiento (GRC)?

Las regulaciones locales están creciendo en volumen y forma, motivo por el cual está aumentando la responsabilidad de los accionistas, funcionarios, ejecutivos y, a su vez la administración de costos relacionados a la gestión de riesgos y cumplimiento, sigue siendo un desafío.

Uno de los desafíos de cumplimiento es la alineación de los procesos de negocio con las normas establecidas por un ente regulador.

La mayoría de las organizaciones consideran las siguientes responsabilidades:

- Continuidad del negocio
- Protección y privacidad de datos

En los últimos años a nivel internacional, se tiene la tendencia a aplicar un modelo GRC, para satisfacer las necesidades y objetivos de una organización.

¿Qué es el modelo GRC?

Es un modelo de gestión que promueve la unificación de criterios, la organización de esfuerzos y la colaboración entre los diferentes involucrados en la dirección de la organización a través de:

- La integración de los órganos responsables del gobierno, la gestión y administración de riesgos, el control interno y el cumplimiento.
- La asignación puntual de roles y responsabilidades del personal clave del proceso de negocio
- La formalización de los canales de comunicación
- La aplicación de un enfoque basado en riesgos
- La implementación de un programa de cumplimiento.(7)

Además, el modelo GRC fomenta el orden de los componentes de la organización para lograr maximizar el valor de las oportunidades y optimizar el rendimiento a través de la gestión de riesgo e incertidumbre, mientras se manteniendo dentro de los límites del cumplimiento con las obligaciones legales y voluntarias. (7)

¿Qué es el desempeño basado en principios?

Es entendido como el logro confiable de objetivos abordando la incertidumbre y actuando con integridad.

El modelo GRC representa un conjunto coordinado e integrado de todas las capacidades necesarias para apoyar el “Desempeño basado en principios”, en toda la organización. (8)

Explicación de los beneficios resultantes del uso de una solución informática GRC

Con el uso de una solución informática para gestionar un modelo GRC se logrará mayor efectividad y eficiencia en el cumplimiento de los objetivos de GRC, así como mayor confiabilidad de los datos, disminución de los costos y una mejor gestión de la complejidad regulatoria.(9)

Con el uso una herramienta informática especializada en gestión GRC se logrará visibilidad al consolidar la información de riesgo y cumplimiento.(10)

Adicionalmente, se obtendrá mayor confiabilidad en los datos porque se configurará el acceso a los mismos mediante funciones de acceso de acuerdo a cada tipo de rol.

Un beneficio adicional que tiene la herramienta informática GRC es que utiliza un flujo de trabajo, intuitivo y muy fácil de usar, para la aprobación de los registros creados y modificados, así como para el control de la integridad de la información. Asimismo, permite notificar a los usuarios, de manera personalizada y amigable, en cada etapa del proceso. (11)

Soluciones tecnológicas GRC existentes en el mercado

IBM OpenPages Policy and Compliance Management

IBM OpenPages Policy and Compliance Management es una solución única que permite a las organizaciones consolidar la gestión de conformidad y políticas, así como gestionar los cambios normativos y la interacción reguladora. El software reduce la complejidad y los gastos asociados al cumplimiento de normas de gobierno, de privacidad, éticas o del sector. (12)

El repositorio de datos único se puede configurar para la clasificación de activos de información. (12)

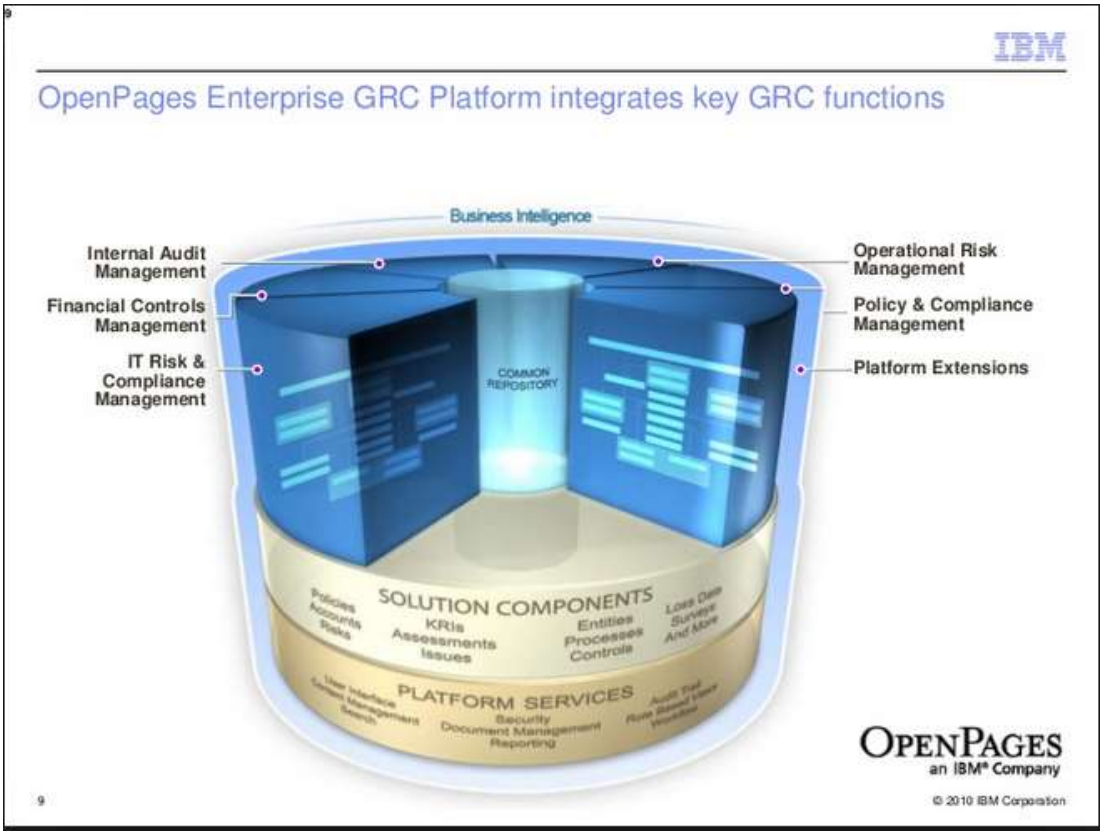


Figura 1 - Solución OpenPages IBM Company

MetricStream GRC

MetricStream es un software que ofrece cumplimiento normativo, gestión de calidad y soluciones de software de auditoría. También ofrece la gestión de activos informáticos, además de permitir la administración, monitoreo y rastreo de los activos para una gestión eficaz del riesgo y de la gestión de TI.(13)

Respecto de la gestión de activos de TI, MetricStream establece que lo más importante de un programa de GRC es crear y mantener un inventario de activos de la organización. Para ello es importante saber qué es lo que hay que proteger y cómo protegerlo.

Generalmente, los datos críticos se encuentran en diferentes ubicaciones de la organización, razón por la cual es necesario conocer las plataformas y el software implementado en el entorno de la red organizacional, de manera de contar con la posibilidad de analizar sus vulnerabilidades y amenazas, permitiendo así la evaluación del riesgo (13)

Figura 2 - MetricStream GRC

Gestar GRC

Es una completa Suite Integral de Soluciones alineada con las mejores prácticas de la industria y el compromiso continuo con las recomendaciones de la ISACA (Asociación de Auditoría y Control de Sistemas de Información) con respecto a los indicadores de gestión apropiados.(14)

Figura 3 - Solución Gestar - Módulos de la plataforma

Incorpora la administración de activos que permite:

1. Identificar los activos
2. Identificar las dependencias entre activos
3. Valorar el activo en cada una de sus dimensiones (14)

Solución RSA Archer eGRC

Figura 4 - Solución RSA Archer - Módulos de la plataforma[3]

Como se puede apreciar en la figura 4, la solución informática RSA Archer cuenta con un módulo denominado Archer Enterprise Management – "Módulo de Gestión Empresarial"; uno de cuyos componentes es el que se utiliza para la automatización del proceso de clasificación de activos. (15)

[3] La plataforma RSA Archer eGRC es una solución tecnológica que incluye los principales componentes de un GRC Empresarial tales como: modelo empresarial, gestión de riesgos, gestión de políticas y controles unificados alineados a la mayoría de estándares y fuentes autoritarias, gestión de continuidad de negocio, gestión de cumplimiento, gestión de incidente, gestión de activos de información, gestión de amenazas, tableros de control y gestión de auditoría.

Capítulo 2 - Metodología e Implementación de la Clasificación de Activos

2.1. Descripción del relevamiento de información del proceso de clasificación de activos de información.

Se utilizará para el desarrollo de este trabajo la consultoría realizada en la entidad financiera "ABC". Para entender la metodología de un cliente es necesario ejecutar el análisis del documento “Blue Print” (BP), el cual contiene sus requerimientos.Este documento fue entregado por el cliente, en concordancia con sus necesidades y requerimientos, a los auditores de una consultora, que de aquí en adelante se denominará “XYZ”. Éstos sostuvieron varias reuniones con los jefes de área de Seguridad Informática y Riesgos de TI de la entidad mencionada, cuyo objetivo fue hacer un relevamiento que recolectara todos los requerimientos del cliente relacionados prioritariamente con el proceso de clasificación de activos.

Después de analizar la herramienta informática GRC y la metodología utilizada por el cliente en el proceso de clasificación activos, se determinó que esa metodología convencional era pertinente pero debía ser optimizada dado que las clásicas hojas de cálculo que le daban soporte eran insuficientes para brindar seguridad a la información.

2.2. Descripción de la metodología de clasificación de la herramienta informática GRC

Cada entidad utiliza su propia metodología para el proceso de “Clasificación de Activos”, ya sea mediante el uso de documentos de cálculo o software para la automatización de este proceso.

Dado que en la actualidad existe una diversidad de procedimientos y tareas que cada entidad financiera realiza de acuerdo con sus intereses particulares y su propia información, para los fines de este trabajo solamente se mostrará cuál es el proceso de clasificación de activos que existe en la

herramienta informática GRC y cómo se puede adaptar según el requerimiento de una entidad financiera en particular.

Se empezará primero a describir la metodología del proceso de clasificación de activos en la herramienta informática GRC, luego se describirá cómo se adaptó la metodología de la mencionada herramienta a la metodología que utilizaba la entidad financiera que nos ocupa.

La metodología de clasificación de activos de información involucra varias aplicaciones de la herramienta informática GRC. Proporciona un repositorio central de información para gestionar las relaciones y dependencias en la jerarquía de negocio y la infraestructura de la organización, que le permite formar una vista en conjunto de las divisiones de la organización, así como determinar el valor de las tecnologías que las soportan, y el uso dela información en el contexto de gobierno, riesgo y cumplimiento (GRC) de toda la organización. (16)

A continuación, se despliega una imagen donde se muestran las relaciones entre las aplicaciones existentes de la herramienta informática GRC.

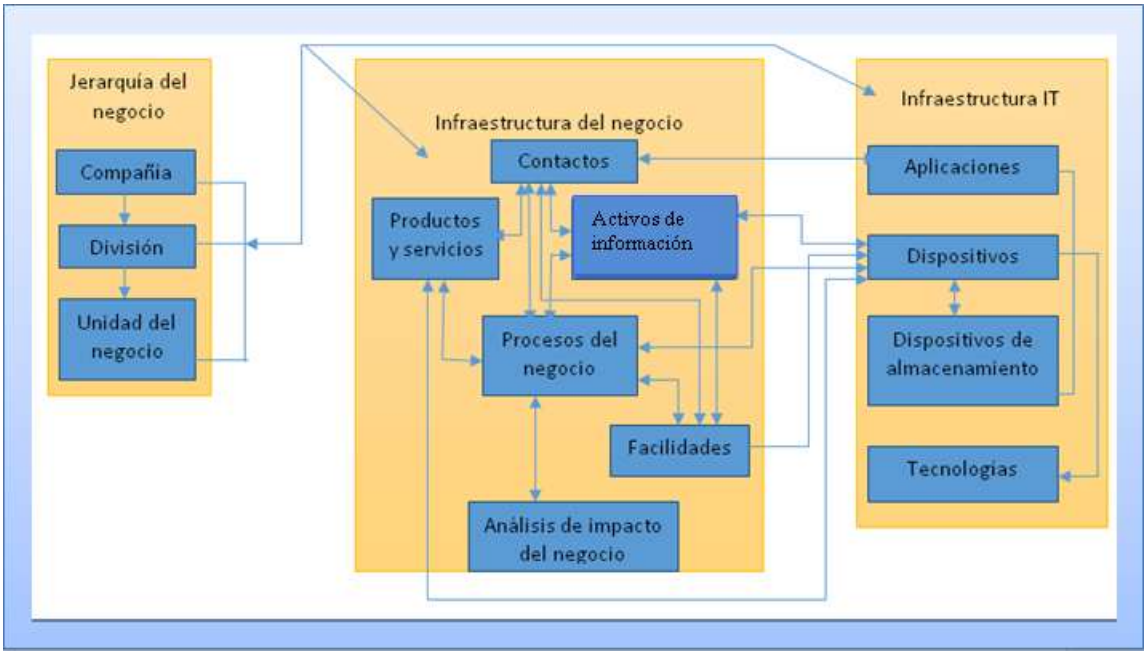


Figura 5 - Relación entre las aplicaciones de la herramienta GRC

2.2.1 Descripción de las aplicaciones del proceso de clasificación de un activo de información en la herramienta informática GRC

El módulo “Enterprise Management” a su vez, está conformado por varias aplicaciones, de las cuales solo algunas de ellas están involucradas en el proceso de clasificación de activos de información, las cuales se describen a continuación:

Aplicación	Descripción
Activos de información	La aplicación de los activos de información contiene información sobre los repositorios de activos de información. Estos almacenes de información pueden contener datos tales como información financiera, registros confidenciales y campos que ayudan a rastrear los fines de su utilización. (16)
Procesos de Negocios	Los procesos de negocio capturan datos relacionados a un determinado proceso incluyendo la información relacionada al impacto en el negocio. Estos procesos pueden estar asociados con las aplicaciones, planes de continuidad, dispositivos y así sucesivamente. (16)

A continuación, mostraremos un diagrama y pasaremos a describir el proceso de clasificación de activos convencional que tiene la herramienta informática GRC.

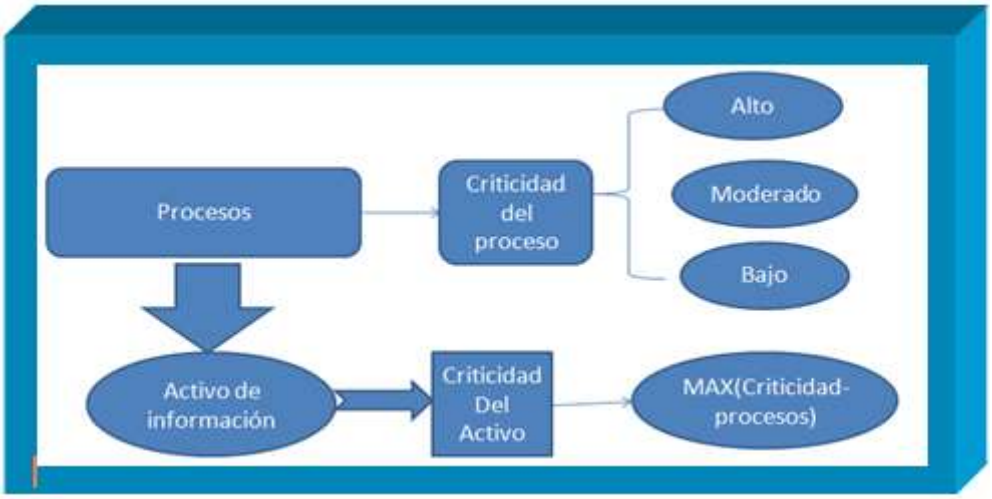


Figura 6 - Proceso de clasificación

En la Figura 6 podemos visualizar que los procesos de negocio están asociados a un activo de información y éstos tienen una criticidad del proceso que puede ser “Alta”, “Moderada” o “Baja”. El activo de información hereda la máxima criticidad de los procesos asociados al activo, la cual utiliza como criticidad del mismo.

Figura 7 - Fórmula del cálculo de la criticidad de un activo

En la figura 7 se muestra la fórmula prediseñada que calcula la criticidad de un activo de información.

2.3.Descripción de la metodología de la clasificación de activos en la entidad “ABC”

Para la entidad financiera “ABC” se hizo una modificación de la manera de obtención de la criticidad para el tipo de activo “Aplicaciones”.

Para entender la metodología utilizada por la entidad fue necesario revisar las directivas que utilizan para el proceso de clasificación de activos tomando en cuenta los siguientes puntos:

- La entidad adopta un modelo CIA (Confidencialidad, Integridad y Disponibilidad) como base para llevar a cabo el proceso de clasificación de activos de información.

- Los tipos de activos involucrados, como así también los responsables de mantener actualizados los componentes que los integran, procediendo a informar los mismos a la Gerencia de Seguridad de la Información con la periodicidad definida dentro de la metodología.

- Los dueños del activo que son los responsables de brindar información acerca del activo del cual están a cargo, deberán realizar una catalogación de los activos que posean asignados en términos de su criticidad y valor para el negocio.

- La clasificación de activos deberá brindar los niveles de criticidad de cada activo de información.

- Otorgar los niveles de acceso a los usuarios para la utilización de la información que debe encontrarse alineada con las criticidades asignados e informados a los activos de información.

- Se debe aplicar mecanismos de control sobre los Activos de Información, basándose para ello en el resultado de la administración de riesgos asociados a los activos de información y el resultado de la Clasificación. (17)

Se analizó los componentes que interactúan en el proceso de clasificación de un activo de información de tipo “Aplicaciones” el cual se ve reflejado en la siguiente imagen:

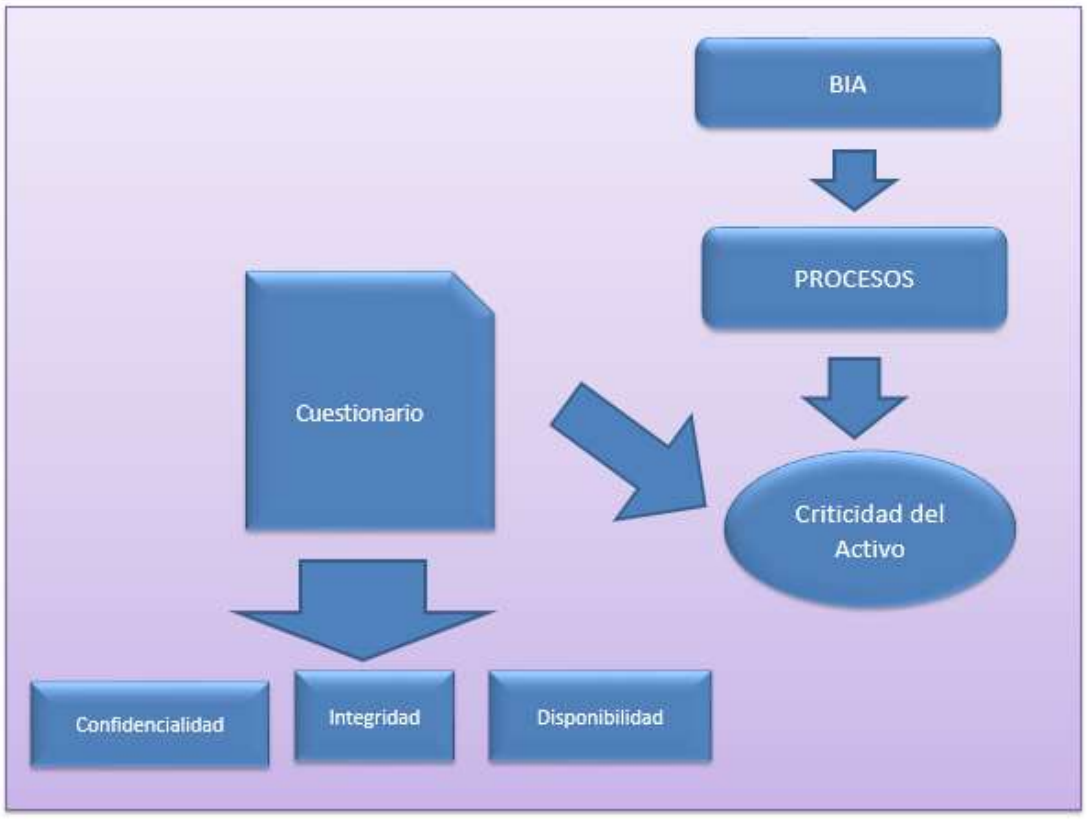


Figura 8 - Metodología del cálculo de la criticidad de un activo de información - Entidad

Los activos están clasificados en niveles. El primer nivel se encuentra integrado por los activos del tipo “aplicativo” incluyendo aquellos específicos del negocio como también los utilizados por las Gerencias de Seguridad de la Información y Tecnología de la Información los cuales denominaremos

aplicativos de tipo “aplicaciones de negocio/soporte” y “aplicaciones de TI”. Este trabajo mostrará cómo se adaptó la metodología a la clasificación de activos de este nivel.

Para determinar la criticidad de los activos de información que pertenecen a este nivel, se empezará describiendo las relaciones entre las aplicaciones y los atributos involucrados en el cálculo de la criticidad del activo.

Según la Figura 8 la relación con la aplicación BIA es a través del resultado del valor del Impacto de cada análisis del negocio que se hace en un tiempo determinado del año. Este valor de Impacto puede ser de tres tipos (3 - Alto, 2- Medio 1 - Bajo), este valor es heredado por el proceso de negocio asociado. Además existe un paso adicional en el cual el dueño del proceso vincula su activo aplicativo con los procesos de negocio en los cuales interviene, estableciendo adicionalmente el tipo de dependencia existente, pudiendo ser la misma del tipo “indispensable” o “soporte”. Una vez establecida la vinculación, se procede a considerar, como uno de los ponderadores para el cálculo de clasificación del activo de información, el valor máximo de criticidad de los procesos asociados. Cabe destacar que los valores de criticidad que poseen asociados los procesos de negocio fueron determinados por la Gerencia de Arquitectura de Procesos y Mejora Continua, basándose para ello en diversos aspectos propios del negocio. Además, cabe mencionar que existen dos cuestionarios específicos para el tipo de activo “Aplicativo”, uno de ellos se encuentra destinado a las aplicaciones de negocio y el otro para aquellas utilizadas exclusivamente por a las Gerencia de Tecnología de la Información y Seguridad de la Información. Ambos cuestionarios se encuentran basados en el modelo CIA (confidencialidad, integridad y disponibilidad), considerándose para los mismos los siguientes criterios.

2.3.1 Criterios definidos para la Confidencialidad

El acceso y/o utilización accidental o desautorizada del activo de información, podría generar alguno de los siguientes consecuencias:

- Acceso sin autorización a información, violando la privacidad y/o las leyes sobre propiedad intelectual.

- Posibles sanciones a la entidad financiera por falta de cumplimiento con los requerimientos de la entidad reguladora BCRA, Habeas Data u otras leyes o normativas vigentes.

- Pérdidas de ventajas competitivas como resultado de exponer información de nuevos productos, posibles fusiones, futuras inversiones, etc.

- Pérdida de clientes, reducción de la imagen de la entidad como resultado de la pérdida de la confidencialidad de información sensible. (17)

2.3.2 Criterios definidos para la Integridad

La modificación o actualización desautorizada de la información contenida en el activo, podría generar alguno de los siguientes consecuencias:

- Pérdida de información valiosa, información de depósitos, cheques, comprometiendo a la entidad o los socios

- Cambios no buscados en sistemas de información, incluyendo aplicaciones, datos y procedimientos que podrían afectar a la integridad de procesos vitales de negocio.

- Demandas legales

- Daño en la reputación, baja en la imagen de la entidad financiera, pérdida de confianza en un mercado potencial. (17)

2.3.3 Criterios definidos para Disponibilidad

La falta de disponibilidad o presencia de los activos de información, accidental o intencional, podría generar alguno de los siguientes consecuencias:

- Una interrupción en la continuidad de los servicios de pagos/aspectos financieros
- Negación de servicios a grandes grupos de clientes con posibles consecuencias(ej. pérdidas financieras sustanciales, demandas legales, pérdidas de clientes)
- Interrupción de procesos de negocio vitales para la entidad
- Publicidad negativa, baja en la imagen de la entidad financiera, pérdida de confianza en un mercado potencial. (17)

2.3.4 Explicación del resultado de la criticidad para cada pilar (CIA)

A continuación se explicará cómo se obtiene la criticidad del activo de tipo aplicación de negocio para cada pilar.

Uno de los parámetros que interviene en el cálculo de la criticidad de cada pilar de un activo, es la sumatoria del puntaje obtenido al completar un cuestionario que está asociado al activo de tipo "aplicación de negocio".

El cuestionario usado para el mencionado cálculo contiene tantas preguntas como requiera una implementación específica. Cada una de ellas está relacionada con un pilar (confidencialidad, disponibilidad e integridad).

Para este ejemplo definiremos un cuestionario de 10 preguntas.

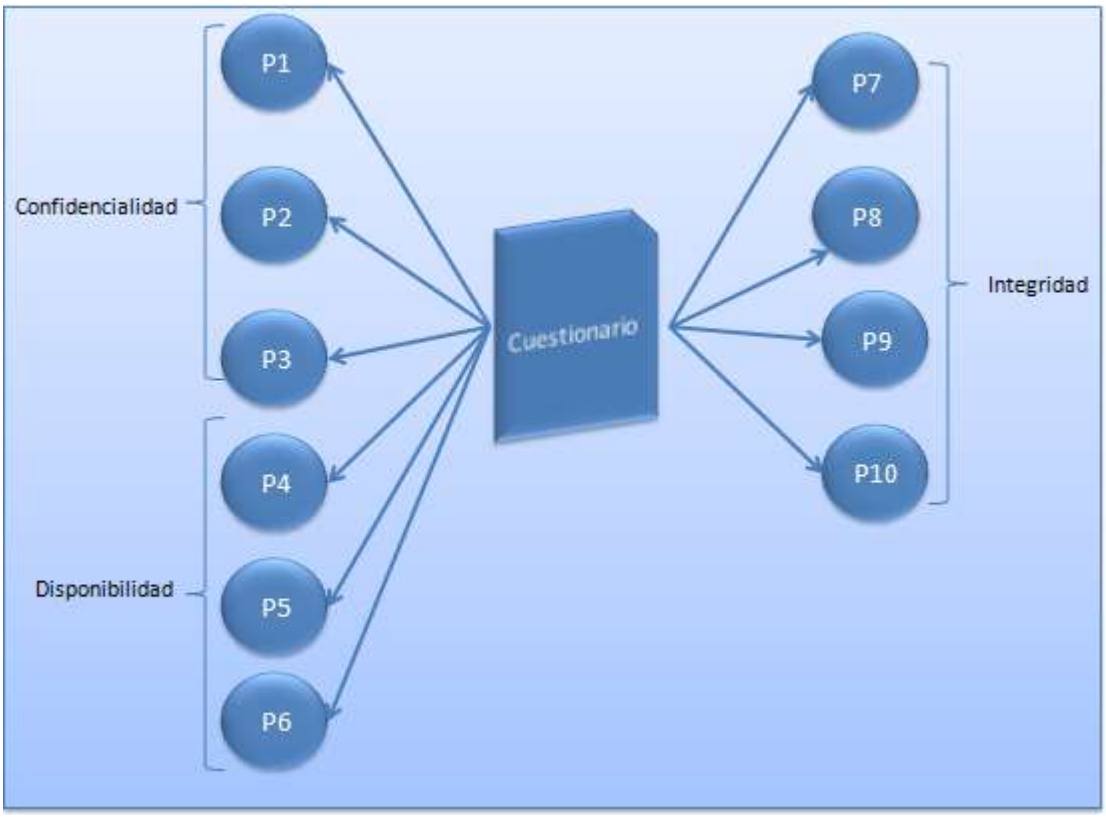


Figura 9 - Cuestionario involucrado en el proceso de clasificación de un activo de información

Tres preguntas están asociadas al pilar de confidencialidad, otras tres están asociadas al pilar de disponibilidad, y las últimas cuatro están relacionadas al pilar integridad.

Cada pregunta del cuestionario tiene un puntaje según la respuesta a la pregunta, la suma del puntaje de las respuestas será el puntaje final para cada pilar.

Confidencialidad – Se obtiene de la suma del puntaje de la respuesta a tres preguntas: P1, P2, P3del cuestionario.

Disponibilidad – Se obtiene de la suma del puntaje de la respuesta a tres preguntas: P4, P5, P6 del cuestionario

Integridad – Se obtiene de la suma del puntaje de la respuesta a cuatro preguntas: P7, P8, P9, P10 del cuestionario.

Después de obtener la suma del puntaje de respuesta para cada pilar, se compara con un parámetro "X" para definir la criticidad por pilar.

Fórmula para calcular el Pilar de Confidencialidad

IF Sumatoria(respuestas pilar confidencialidad) > X → Alto

IF Sumatoria(respuestas pilar confidencialidad) = X → Medio

IF Sumatoria(respuestas pilar confidencialidad) < X → Bajo

Fórmula para calcular el Pilar de Disponibilidad

IF Sumatoria(respuestas pilar disponibilidad) > X → Alto

IF Sumatoria(respuestas pilar disponibilidad) = X → Medio

IF Sumatoria(respuestas pilar disponibilidad) < X → Bajo

Fórmula para calcular el Pilar de Integridad

IF Sumatoria(respuestas pilar integridad) > X → Alto

IF Sumatoria(respuestas pilar integridad) = X → Medio

IF Sumatoria(respuestas pilar integridad) < X → Bajo

2.3.5 Descripción de la metodología con ponderaciones para el cálculo de la criticidad del activo de primer nivel

El proceso de clasificación de activos empieza con el resultado que proviene del valor del impacto que puede ser cada uno de ellos con una diferente ponderación:

Alto- > 3

Medio-> 2

Bajo->1

La ponderación del impacto es heredado por los procesos de negocio que tiene asociado cada BIA. Los procesos de negocio a su vez tienen aplicaciones asociadas.

El cálculo de la criticidad de un activo proviene del resultado del promedio de los pilares (confidencialidad, integridad y disponibilidad) y del máximo valor del impacto del proceso asociado al activo.

Capítulo 3 Implementación del proceso de clasificación de activos en la herramienta informática GRC

3.1 Descripción de las aplicaciones utilizadas para la implementación del proceso de clasificación de activos

Las aplicaciones del software original que venían en la herramienta GRC eran insuficientes para cumplir con la metodología de clasificación de activos del cliente, por los cual se personalizo la aplicación de activos de información dividiéndola en dos, una de ellas de “Asignación de dueño del activo” y otra para la “Clasificación de activo”. De igual forma, se personalizó la aplicación “Aplicaciones”.

A continuación, se muestran las aplicaciones que fueron personalizadas para el proceso de la clasificación de activos.

Aplicación	Descripción
Activos de información	Se niveló la aplicación en 2 niveles: **Asignación del responsable del activo:** Esta aplicación tiene la función de asignación de un dueño y especialista de un activo. **Clasificación de activos:** Esta aplicación tiene la función de clasificar los activos según los procesos asociados y la encuesta de evaluación del activo.
Aplicaciones	La aplicación almacena información acerca de las aplicaciones empresariales utilizadas en la organización, pueden ser de dos tipos: aplicaciones de negocio y de tecnología de la información, además tiene un resumen de todas las clasificaciones que se hicieron a la aplicación.

3.2 Descripción de la creación del cuestionario para la aplicación “aplicaciones” en la herramienta informática GRC

A continuación, se muestran los atributos que serán creados en el cuestionario.

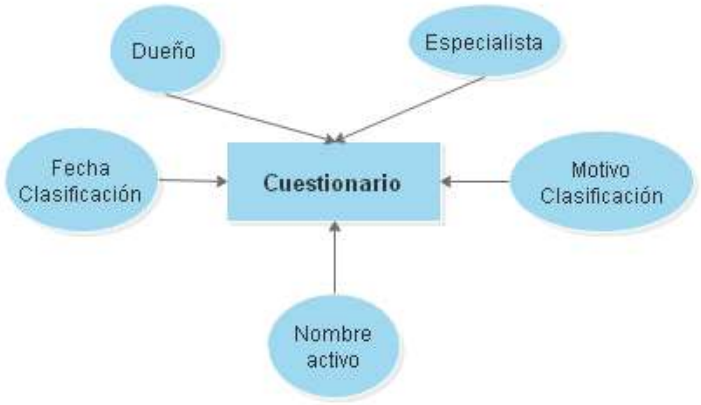


Figura 10 - Atributos de la aplicación "Cuestionario"

En la figura 10 podemos observar los siguientes campos:

Dueño: Nombre del dueño del activo de información.

Especialista: Nombre del especialista del activo de información.

Fecha de clasificación: Indica la fecha de creación del cuestionario.

Motivo de clasificación: Indica el motivo por el cual se clasifica el activo de información.

Nombre activo: Indica el nombre del activo de información.

Se empezó con la personalización de las encuestas tomando como referencia las aplicaciones de tipo cuestionario, que vienen incorporadas en la herramienta informática GRC. Luego, se continuó personalizando cada una de las encuestas de acuerdo con los formatos presentados en el requerimiento. Después de esta etapa, se inició la digitalización de las preguntas en cada una de las aplicaciones de tipo encuesta.

Fue preciso revisar el formato del documento entregado por el cliente con el objeto de elegir un conjunto de preguntas que, posteriormente, fueron trasladadas al cuestionario personalizado de la herramienta. Además, el cuestionario fue sometido a la automatización para que funcione con un flujo de aprobación.

Para llevar a cabo el proceso de personalización se toma un conjunto de preguntas que se transcriben en el cuestionario personalizado de la herramienta. Además, este cuestionario se personaliza con el objetivo de que en su funcionamiento intervenga un flujo de aprobación. En este esquema interactúan los siguientes roles:

- Grc_Dueño
- Grc_Especialista
- Grc_Clasificador

El cuestionario tiene un flujo de trabajo para aprobación, el cual describiremos a continuación:

Para entender el flujo de trabajo definiremos algunos términos:

N1: Notificación enviada desde el sistema al rol GRC_Dueño

N2: Notificación enviada desde el sistema al rol GRC_Especialista

R1: Notificación de parte del rol GRC_Dueño al rol GRC_Especialista

R2: Notificación de rechazo de parte del rol GRC_Dueño al rol GRC_Especialista

Como se dijo más arriba, en el esquema de aprobación interactúan los roles de **Grc_Dueño**, **Grc_Especialista**, **Grc_Clasif**. El flujo empieza cuando crea un cuestionario para el rol Grc_Clasif, luego se envía un mail al rol Grc_Dueño del activo quien completa el cuestionario, el cual se aprueba automáticamente. Asimismo, hay una segunda opción que consiste en derivarlo a un especialista encargado de completar el cuestionario. Luego,

se envía un mail informando al dueño que el cuestionario fue completado por el especialista; finalmente, el dueño aprueba o rechaza el cuestionario que completó el especialista.

3.2.1 Flujo de trabajo del Cuestionario de Aplicaciones de Negocio

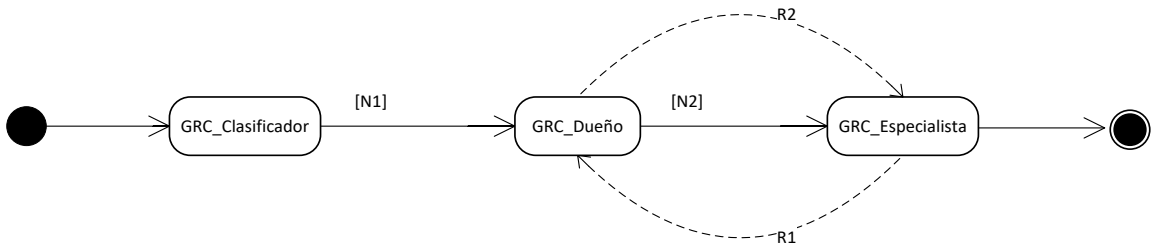


Figura 11 - Flujo de trabajo del cuestionario de aplicaciones de negocio

3.2.2 Descripción del Flujo de trabajo para la aprobación de Aplicaciones de Negocio

1. <u>Curso Normal</u>. (Creación de un cuestionario aprobado por el dueño.)

a. El analista de clasificación crea un cuestionario de "aplicación de negocio", completa la información correspondiente al tipo de clasificación del activo y elije una fecha para esa clasificación.

b. Después de que el analista hace este procedimiento, el sistema, de manera automática, dispara un mail N1 cuyo destinatario es el dueño del activo, quien se encarga de completar el cuestionario al que accede a través del enlace que recibe en la notificación N1.

c. El cuestionario se aprueba automáticamente cuando el dueño del activo responde las preguntas del mismo.

d. Se envía una notificación al analista de clasificación de activos con copia al dueño del activo, informando que el cuestionario fue

completado por el dueño del activo y está listo para proceder con la clasificación del activo de información.

2. **Curso Alternativo. Cuestionario Derivado.**

a. El analista de clasificación crea un cuestionario de aplicación de negocio, completa la información correspondiente al tipo de clasificación del activo y elije una fecha para esa clasificación.

b. Envía una notificación N1 al dueño del activo para hacerle saber que está pendiente completar el cuestionario del activo de información

c. El dueño ingresa al cuestionario y deriva a un especialista para que pueda completarlo.

d. Se envía una notificación N2 al especialista, informando que tiene pendiente completar el cuestionario del activo de información

e. El especialista ingresa al cuestionario y responde las preguntas.

f. Se envía una notificación al dueño del activo, informando que el especialista completó el cuestionario del activo de información.

g. El dueño ingresa a revisar el cuestionario y aprueba el mismo.

h. Se envía una notificación al analista de clasificación de activos con copia al dueño del activo, informando que el cuestionario fue completado por el dueño del activo y está listo para proceder con la clasificación del activo de información.

3. **Curso Alternativo. Cuestionario Rechazado**

a. El analista de clasificación crea un cuestionario de "aplicación de negocio", completa la información correspondiente al tipo de clasificación del activo y una fecha.

b. Se envía una notificación N1 al dueño, informando que tiene pendiente completar el cuestionario del activo de información.

c. El dueño ingresa al cuestionario y deriva a un especialista para que pueda completarlo.

d. Se envía una notificación N2 al especialista, informando que tiene pendiente completar el cuestionario del activo de información.

e. El especialista ingresa al cuestionario y responde las preguntas.

f. Se envía una notificación al dueño del activo, informando que el especialista completó el cuestionario del activo de información.

g. El dueño ingresa a revisar el cuestionario y rechaza el mismo.

h. Se envía una notificación R2 al especialista, informando que tiene pendiente revisar el cuestionario del activo de información.

i. Se envía una notificación al dueño R1 del activo, informando que el especialista completó el cuestionario del activo de información.

j. El dueño ingresa a revisar el cuestionario y aprueba el mismo.

k. Se envía una notificación al analista de clasificación de activos con copia al dueño del activo, informando que el cuestionario fue completado por el dueño del activo y está listo para proceder con la clasificación del activo de información.

3.3 Configuración de acceso a los roles y perfiles

Antes de empezar a describir la configuración de roles y perfiles en la herramienta informática GRC, los definiremos**.**

¿Qué es un Rol?

"*El Rol es el nombre que se le otorga al conjunto de perfiles que son asignados al usuario para el ejercicio de sus funciones.*"

"*Es una entidad especial para ejecutar aplicaciones con privilegios. Sólo los usuarios pueden asumir la entidad especial.* **"**(18)

¿Qué es un Perfil?

"*Es la descripción detallada de las posibles acciones (lectura, escritura, eliminación, actualización) que puede realizar un usuario en el sistema.*"

"*Es una recopilación de capacidades administrativas que se pueden asignar a un rol o a un usuario. Un perfil de derechos puede constar de autorizaciones, comandos con atributos de seguridad y otros perfiles de derechos.*"(18)

El estándar ISO/IEC 27002:2013 define en el punto 9.1. el objetivo de control "Requisitos del negocio para el control de acceso" como: Limitar el acceso a la información y a las instalaciones de procesamiento.

En el punto 9.1.1 "Política de control de acceso" el estándar indica que se debería establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad de la información. Para su implementación se debería determinar apropiadas reglas de control de acceso, permisos y restricciones para cada rol de usuario específico. Asimismo establece que los controles de acceso son tanto lógicos como físicos y éstos deberían ser considerados juntos.

Según la política, se considera importante para el control de acceso los siguientes puntos:

- Consistencia en el control de acceso y las políticas de clasificación de la información de los diferentes sistemas y redes.
- Los perfiles de acceso de usuario estándar para puestos de trabajo comunes en la organización.
- Segregación de roles de control del acceso; por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso.

Según el control 9.2.3 "Gestión de privilegios", éstos se deberían asignar a los usuarios sobre la base de "sólo lo que necesita saber" y sobre una base de evento-por-evento, en línea con la política de control de acceso (9.1.1). Es decir, se le asignarán los requerimientos mínimos para su rol funcional.

Tomando en cuenta la normativa y los controles enunciados anteriormente podemos concluir que la herramienta informática GRC se alinea con las políticas especificadas con el estándar internacional ISO/IEC 27002:2013.

Ahora mostraremos una breve descripción de la configuración de los perfiles y roles que son usados en el proceso de “clasificación de activos”. La herramienta informática GRC muestra un marco donde se pueden configurar los perfiles según los roles creados.

Figura 12 - Configuración de perfil de acceso a las aplicaciones

En la Figura 12 vemos que se asignaron permisos de lectura y actualización sobre la aplicación “Cuestionario de Aplicaciones de Negocio”. para el rol de dueño del activo.

3.4 Proceso de clasificación de un activo de información en la herramienta informática GRC

Se mostrará un caso práctico del proceso de clasificación de activos utilizando la herramienta informática GRC. En él se considerará un activo de tipo "aplicación de negocio" identificado como “ISOL – I-Sol”, el cual está asociado a dos procesos de negocio denominados P1, P2.

3.4.1 Paso a Paso del proceso de clasificación de activos del activo de información “ISOL –I- Sol”

1. El usuario clasificador de activos (GRC_Clasificador) ingresa a la plataforma con su usuario y contraseña, luego selecciona la opción “*Activos de Información*” en el menú lateral izquierdo.
2. El usuario clasificador (GRC_Clasificador) selecciona la opción “Clasificación de Activos”. (Anexo I - fig. 15)
3. El usuario clasificador (GRC_Clasificador) selecciona el tipo de clasificación “Aplicaciones de Negocio/Soporte” (Anexo I - fig. 16)
4. El usuario clasificador busca el activo de información “ISOL – I- SOL”. (Anexo I - fig. 17)
5. El usuario clasificador (GRC_Clasificador) selecciona el activo de información “ISOL – I- SOL” un activo de información. (Anexo I - fig. 18)
6. El usuario clasificador selecciona los procesos asociados al activo. (Anexo I - fig. 19)
7. El usuario clasificador (GRC_Clasificador) agrega un nuevo cuestionario. (Anexo I - fig. 20)
8. El usuario dueño del activo completa el cuestionario para el activo “ISOL –I-SOL” (Anexo I - fig. 21)

9. Se muestran los resultados de la criticidad del activo y la criticidad de cada pilar del activo de información “ISOL- I-SOL”. (Anexo I - fig. 22)

Después de obtener el resultado de la criticidad del activo es necesario darla a conocer a los responsables del activo, los cuales son: el dueño del activo y el especialista del activo. Esta información es enviada por el responsable de la clasificación del activo por medio de una notificación después de terminar el proceso de clasificación del activo.

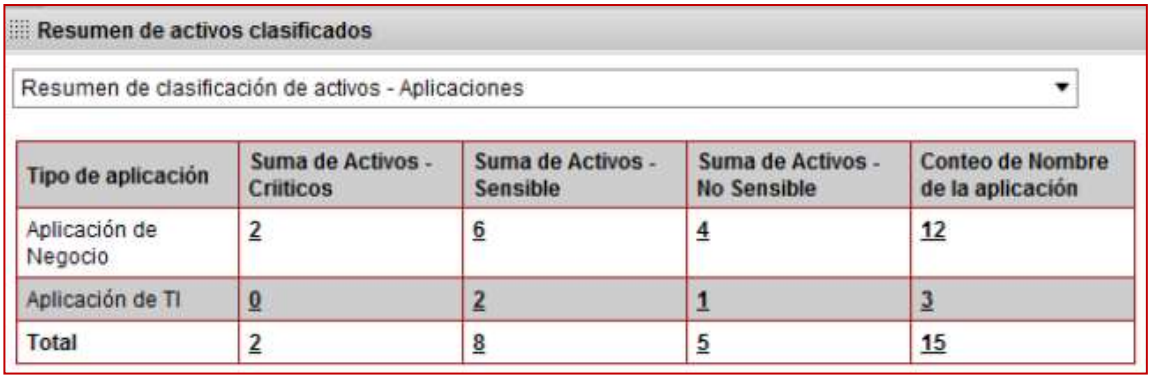
Además, dependiendo del resultado de la criticidad del activo se maneja un cronograma para su reclasificación. El cuál se describirá a continuación:

Si la clasificación de un activo da por resultado que es "crítico" se volverá a realizar el proceso de clasificación cada tres meses; si es "sensible" se clasificará cada seis meses; de lo contrario se reclasificará cada doce meses.

3.5 Informes obtenidos después del proceso de clasificación de activos

Una vez finalizado el proceso de clasificación de activos es posible evidenciar que los resultados obtenidos agregan valor o sirven como entrada (ingreso) para el proceso de autoevaluación de riesgos de un activo de tipo "aplicación de negocio". Dicho proceso consiste en evaluar el riesgo que ese activo tiene para la organización, según el resultado de criticidad obtenido para el mismo.

Estos reportes presentan de manera resumida y ordenada los resultados de la clasificación de activos de tipo "aplicación de negocio", los cuales sirven para tomar medidas de seguridad según la criticidad de los mismos. A continuación se muestran algunos reportes con los resultados obtenidos.



Resumen de activos clasificados

Resumen de clasificación de activos - Aplicaciones

Tipo de aplicación	Suma de Activos - Criiticos	Suma de Activos - Sensible	Suma de Activos - No Sensible	Conteo de Nombre de la aplicación
Aplicación de Negocio	2	6	4	12
Aplicación de TI	0	2	1	3
Total	2	8	5	15

Figura 13 - Reporte de resumen de clasificación de activos – aplicaciones

1. En el reporte de la figura 13 se puede apreciar la cantidad de activos de acuerdo con su nivel de criticidad. En relación con éste los activos se clasifican en críticos, sensibles y no sensibles. Esta clasificación proporciona la base para la protección de dichos activos. Un activo se clasifica como crítico cuando es susceptible a altos factores de riesgo; se dice que es sensible si se encuentra en condiciones de riesgo medio y se determina como no sensible si las posibilidades de ser afectado o sufrir riesgo es baja.

Sobre la base de estos parámetros clasificatorios fueron consideradas las aplicaciones de tipo “Aplicaciones de TI” y Aplicaciones de Negocios.

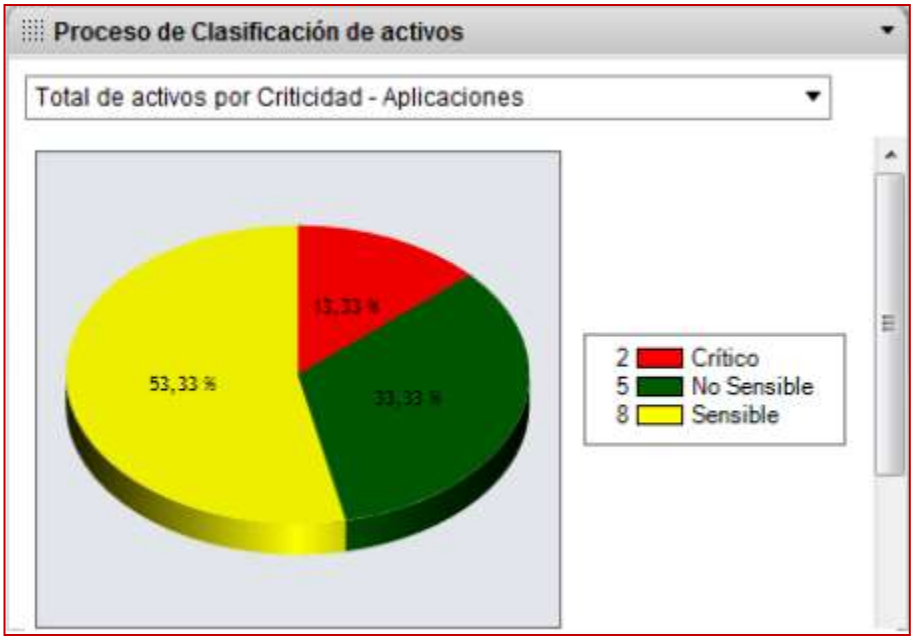


Figura 14 - Reporte del porcentaje de la criticidad de las aplicaciones

2. En concordancia con la clasificación ya expuesta, en la figura 14 se observa el porcentaje de los activos críticos, sensibles y no sensibles, de los activos de tipo aplicaciones de negocio. Además se deduce la proporción de activos críticos para poder darle el resguardo correspondiente. La utilidad de este reporte radica en evidenciar la cantidad de activos críticos que demandan una evaluación pertinente de riesgos del activo, y de esta manera determinar la implementación de controles precisos para mitigar el riesgo.

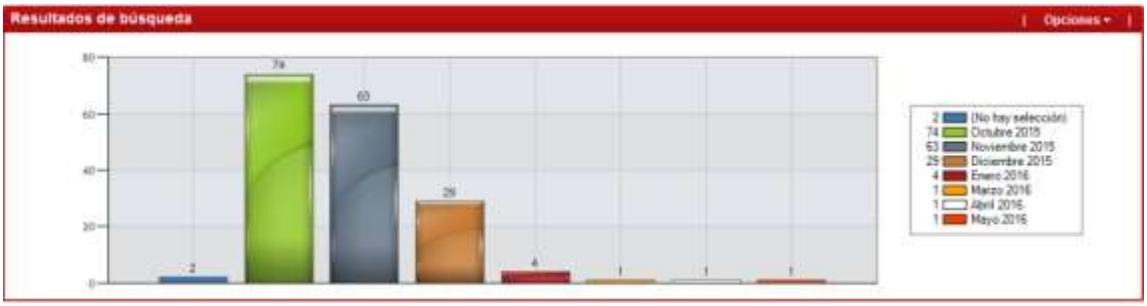


Figura 15 - Reporte de la cantidad de activos clasificados por mes

3. En la figura 15 se presenta un reporte que provee información relacionada con la cantidad de activos clasificados por mes. De esta manera es posible observar que el más alto porcentaje de activos fue clasificado en el mes de Noviembre de 2015, y que en el mes de Mayo de 2016, como periodo de tiempo más reciente, se dio conocimiento de un solo activo clasificado.

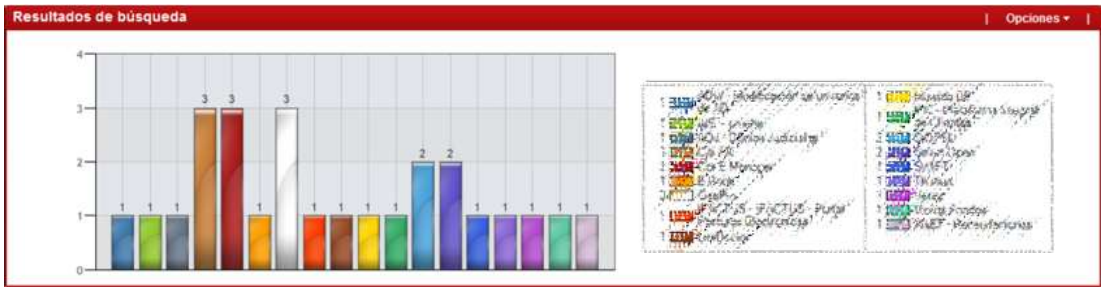


Figura 16 - Reporte de la cantidad de veces que se clasifico un activo de información

4. La figura 16 proporciona valiosos datos relacionados con el reporte que hace evidente la frecuencia o cantidad de veces en que clasificó un activo de información durante el periodo de un año. Tomando en cuenta que los activos críticos fueron clasificados con más frecuencia que el activo sensible o no sensible, podemos observar cuáles activos tienen una alta criticidad y cuáles tienen una criticidad media o baja.

Conclusiones

La implementación finalizó con una interfaz amigable que permitió al usuario agilizar sus procesos, aunque el proyecto sufrió retrasos y desvíos en el calendario, que se presentaron en más de una oportunidad.

Se implementó una interfaz segura dado que anteriormente el proceso se llevaba en hojas de cálculo que podían ser fácilmente modificadas. Es decir, la información era susceptible a alteraciones por parte de terceros, razón por la cual, los datos podrían no ser fidedignos ni representar una realidad concreta, un universo exacto de datos, para el proceso de autoevaluación de riesgos.

Los beneficios obtenidos tras el proceso de clasificación de activos son múltiples empezando por la posibilidad de obtener resultados exactos respecto de activos críticos, sensibles y no sensibles, así como la de brindar una interfaz segura, amigable en su manejo y que engloba o une todos los procesos en una plataforma. De esa manera, es posible tener una visión global de los procesos que interactúan con el proceso de clasificación de activos y contar con notificaciones automáticas. Además de toda la experiencia adquirida, esta implementación permitió el trabajo en equipo con las personas responsables de la clasificación de activos y así entender cómo es el proceso, más allá de lo conceptual; comprendiendo cómo esto ayuda a las personas y les da otra perspectiva de manejo y ahorro de tiempo.

Es preciso destacar la importancia de que estos resultados son de valor agregado para los usuarios, que son esenciales para su desempeño y que a su vez permiten a la Alta Gerencia tomar decisiones en cuanto a la efectiva y eficaz administración de los riesgos de los activos que fueron clasificados.

Anexo I

Figura 17 - Opciones de la aplicación de activos de información

Figura 18 - Opción de selección del tipo de aplicativo

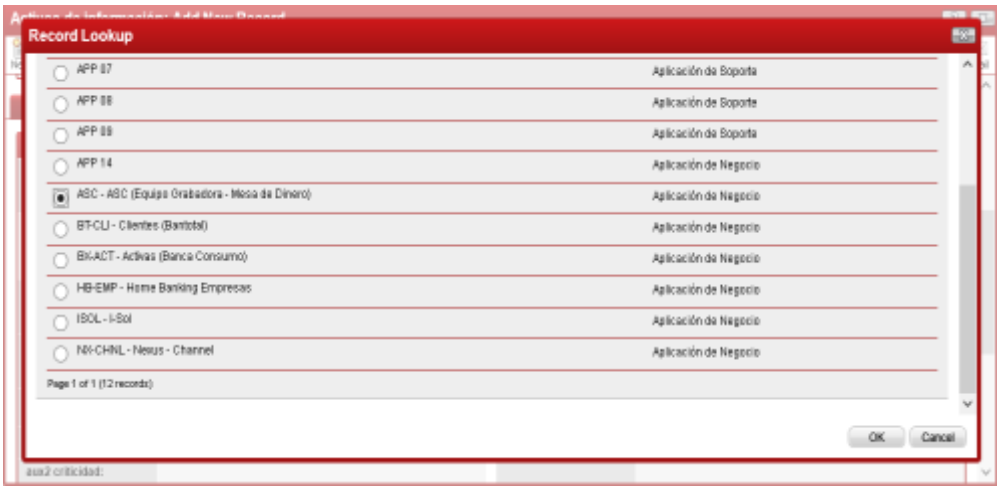


Figura 19 - Listado de aplicaciones de Negocio/Soporte

Figura 20 - Aplicativo seleccionado

Figura 21 - Listado de procesos asociados al activo BT-CLI

Figura 22 - Ventana para la creación de un cuestionario

Figura 23 - BT-CLI cuestionario seleccionado

Figura 24 - Resultado de la clasificación del activo BT-CLI

Bibliografía

[1]. Siete consideraciones al evaluar herramientas GRC automatizadashttp://searchdatacenter.techtarget.com/es/consejo/Siete-consideraciones-al-evaluar-herramientas-GRC-automatizadas (Consultada 26/08/2015)

[2]. Las compañías pierden un tiempo muy valioso en funciones que eGRC puede resolver.http://www.redseguridad.com/empresas/fabricantes/las-companias-pierden-un-tiempo-muy-valioso-en-funciones-que-egrc-puede-resolver(Consultada 27/08/2015)

[3]. Harold F. Tipton, Micki Krause, Information Security Management Handbook, New York, 2007

[4]. Argentina BCDLR. COMUNICACIÓN "A" 4609.http://www.bcra.gov.ar/pdfs/comytexord/A4609.pdf(Consultada30/07/2016)

[5]. Strategist SSG. Charlotte ISACA Risk Intelligence - 6-3-14. http://www.isaca.org/chapters3/Charlotte/Events/Documents/Event%20Presentations/06162014/Charlotte%20ISACA%20Risk%20Intelligence%20-%206-3-14.pdf (Consultada 30/07/2016).

[6]. Ruiz F. Procesos de Negocio y Desarrollo de SW. http://alarcos.esi.uclm.es/per/fruiz/curs/santander/fruiz-pn.pdf(Consultada17/09/2016).

[7]. Deloitte. Servicios de Gobierno, Riesgo y Cumplimiento(GRC) –Soluciones integrales a la medida de sus necesidades - https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/mx(es-mx)ServiciosGRC.pdf (Consultada20/07/2016).

[8]. Carole S. and Switzer C.,Modelo de Capacidad de GRC, Creative Commons-Share Alike 3.0, United States, 2015.

[9]. Daniel Claudio Vita. Pasos Prácticos para la Implementación de una Solución Informática como soporte al Modelo GRC. - Novared - 2015.

[10]. Rouse M. Software de GRC (gobernanza, gestión de riesgos y cumplimiento) - http://searchdatacenter.techtarget.com/es/definicion/Software-de-GRC-gobernanza-gestion-de-riesgos-y-cumplimiento (Consultada02/07/2016).

[11]. Corporation E. RSA Archer GRC Plataform – Automate, integrate,manage and

report across your enterprise -https://www.emc.com/collateral/data-sheet/11151-egrcp-ds.pdf(Consultada02/08/2016).

[12]. IBM OpenPages and Compliace Management http://www-03.ibm.com/software/products/es/openpages-policy-compliance-management/.(Consultada 03/03/2017)

[13]. 2017 MetricStream Enterprise Risk Management App.

http://www.metricstream.com/apps/enterprise-risk-management.htm (Consultada 03/03/2017)

[14].
2016 Soto A. IT Gobernance. http://www.gestar.com/soluciones/grc (Consultada 01/30/2017)

[15]. Sarah Adams GLCRSSER., Governance, Risk and Compliance, In Specialist O. editor, ISACA Monterrey, 2013

[16]. EMC C. RSA Archer eGRC Suite - RSA Archer Enterprise Management - In EMC C. RSA Archer eGRC Suite. USA; 2012. p. 17.

[17]. Financiera E. Política de Inventario y Clasificación de Activos de Información. - Documento de la entidad "ABC"

[18]. Oracle y/o Subsidiarias - Guía de administración del sistema: servicios de seguridad -https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html(Consultada 11/10/2016).

[19]. EMC C. RSA Archer GRC Platform 5.4. 2013. p. 8-9.

[20]. Asteasuain F., UML Lenguaje Unificado de Modelado,Computer Science Department. School of Science UBA, Buenos Aires, 2009

[21]. Archer RG. Manage Risk and Compliance with Rapid7 Nexpose and Archer GRC -https://www.rapid7.com/(Consultada07/30/2016).

[22]. Deloitte. En la misma dirección, uniendo al Gobierno, Riesgo y Cumplimiento(GRC) - http://www.isaca.org/chapters7/Monterrey/Events/Documents/20101206%20Uniendo%20al%20Gobierno%20(GRC).pdf(Consultada20/07/2016).

[23]. Informática UMeS. Gestión Estratégica de la Seguridad - Gestión de activos. 2013.

[24]. Rouse M. Software de GRC (gobernanza, gestión de riesgos y cumplimiento) - http://searchdatacenter.techtarget.com/es/definicion/Software-de-GRC-gobernanza-gestion-de-riesgos-y-cumplimiento (Consultada02/08/2016).

[25] 2016 Gartner A. Positioning Technology Players Within a Specific Market - http://www.gartner.com/technology/research/methodologies/research_mq.jsp(Consultada10/10/2016).

[26]. 2015 Alonso C. SandaS & Sandas GRC: Gestión y Gobierno de la Seguridad http://www.elladodelmal.com/2015/09/sandas-sandas-grc-gestion-y-gobierno-de.html Consultada(2017/03/01)

[27]. 2017 Cumplimiento GGTI. GESDATOS Software. http://www.gesconsultor.com/ens/valoracion.html.Consultada(01/03/2017)