Proyecto Final de Carrera

Memoria técnica de proyecto:

Technology Governance Risk and Control

UTN SANTA FE

CARGILL ENGINEERING

Cargill Helping the world thrive

Aclaración: El autor no posee ningún derecho sobre las imágenes, logos o cualquier otra referencia a la empresa, los mismos son, sólo, a modo de contextualizar mejor el trabajo del autor en la empresa durante ése período

Autor: Claudio Gerarduzzi

Carrera: Ingeniería en Sistemas

Año: 2018

ÍNDICE

AGRADECIMIENTOS 5
1 INTRODUCCIÓN 6
1.1 Contextualización 6
1.2 TGRC como Necesidad o Fundamento del Proyecto 7
1.3 TGRC, Por Qué Necesitamos Gestionar el Riesgo Tecnológico? 8
1.4 El Abordaje de la Empresa a los Riesgos en la Tecnología 9
1.5 TGRC y su MISION 10
1.6 TGRC y su Organización Central en la Empresa de Referencia 10
1.7 TGRC y su Plataforma 12
1.9 TGCR, Mapa de Despliegue 14
2 POLITICAS DE TGRC, MISION DE LA EMPRESA Y PLAZOS DEL PROYECTO 17
2.1 Políticas y su Alcance 17
2.2 Declaración General de Políticas sobre la Información 18
2.3 TGRC, Centro de Terminología de Política 19
2.4 Dónde son Almacenadas las Políticas? 22
2.5 Misión, Visión y Principios Guías 23
2.6 Plazos de Ejecución 24
3 MÉTRICAS 26
3.1 Qué son las Métricas? 26
3.2 Necesidad de Métricas 27
3.3 Tablero de Control o Scorecard 28
3.4 Elaboración del Tablero de Control o Scorecard 28
3.5 Ejemplo de Datos del Scorecard o Tablero de Control 29
3.6 Proceso de Comunicación de las Métricas en TGRC 34
3.7 Roles y Responsabilidades 35
3.8 Software Encargado en de Recolectar Datos 36
4 ARCHER 37
4.1 Introducción al Software 37
4.2 Aproximación de Archer a TGRC 38
4.5 Principales Funcionalidades 41
4.6 Modo de Utilización 42
4.7 Formato Gráfico 43

4.8 Ruta de Acceso al Proceso de la Organización 45
5 IDENTIFICACIÓN DE PROCESOS Y SUBPROCESOS 47
5.1 La razón por la que definimos Procesos y Subprocesos 47
5.2 Diseño Descendente Orientado a Procesos 48
5.3 Reingeniería de Procesos, la Apuesta de la Empresa 49
5.4 La Apuesta de TGRC al Usar la Metodología 50
5.5 TGRC y los Pasos en la Identificación 51
5.6 TGRC y los Procesos Preestablecidos 52
5.7 Tecnología Usada por Proceso 55
5.8 TGRC y la Simplificación de Procesos 55
5.9 TGRC y la Valoración de los Procesos 56
6 COORDINAR LAS ACTIVIDADES 59
6.1 Coordinar y su Implicancia en Proyectos 59
6.2 Coordinar las Actividades de Riesgo y Control 60
6.3 Principales Áreas de Riesgo (KRAs) 62
6.4 Encontrar las Principales Áreas de Riesgo (KRAs) Dentro de la Empresa 62
6.7 Relaciones Entre la Actividad RCC y las KRAs 64
6.8 Identificación y Entrenamiento de los Coordinadores de Riesgo y Control en la BU/Función 65
6.9 Coordinación del Entrenamiento de los Usuarios 66
6.10 Coordinación de las Caminatas de Control o WALKTHROUGH 67
7 COORDINACIÓN DE RIESGOS PURAMENTE TECNOLÓGICOS 69
7.1 Coordinar las Actividades de Control de Riesgos Específicamente Tecnológicos 69
7.2 Relación Entre la Actividad TRCC y las KRAs 70
7.3 Coordinación en Parches de Seguridad y Antivirus 71
7.4 Tablero de Control o Scorecard de TGRC y su Rol en la Coordinación 71
7.5 Coordinación en la Evaluación del Software 72
7.6 Coordinación en la Revisión de los Accesos Lógicos 72
7.7 Coordinación de Ciclo de Vida del Hardware 75
7.8 Coordinación en los Acuerdo de Acceso a la Red (NAA) y Evaluación del Riesgo (NCRA) 75
8 PLAN DE CONTINGENCIAS o RESILIENCY MANAGEMENT PLAN 77
8.1 La Necesidad de un Plan de Contingencias en la Empresa 77

8.2 Componentes del Plan de Gestión de Contingencias o Resiliency Management 79
8.3 Análisis de Impacto de Negocio o Business Impact Analysis (BIA) 80
8.4 Plan de Continuidad de Negocio o Business Continuity Plan (BCP) 86
8.5 Plan de Recuperación de Desastres (DRP) 92
8.6 Planificación de Gestión de la Crisis (CMP) 95
8.7 Plan de Pruebas o Tests 96
9 CONCLUSIONES 97
9.1 Consideraciones Generales del Proyecto TGRC, su Relación con la Organización 97
9.2 Consideraciones Generales del Proyecto TGRC, las Percepciones del Autor 99
9.3 Consideraciones Generales del Proyecto TGRC, Principales Desafíos 100
ANEXO I: ROLES 102
- RCC/TRCC/SRCC 102
- TECHNOLOGY RISK AND CONTROL COORDINATOR 104
- SITE RISK AND CONTROL COORDINATOR 106

ANEXO II: EJEMPLO DE MODIFICACIÓN REQUERIDA PARA USAR ARCHER CON WINDOWS POWER SHELL 108
ANEXO III: DESARROLLO BIA 111
ANEXO IV: LISTA DE ACRÓNIMOS 114
ANEXO V: ÍNDICE DE FIGURAS Y TABLAS 115
ANEXO VI: BIBLIOGRAFÍA 116

AGRADECIMIENTOS

En agradecimiento a mi familia, a mi esposa e hijos que estuvieron siempre presente en los momentos buenos y adversidades, sobre todo acompañando especialmente al retomar los estudios. Desafío que no resultó fácil, no solo por el tiempo perdido sino por todas las responsabilidades que demanda ahora familia y trabajo. También agradezco a los profesores que me acompañaron, formaron y apoyaron tanto en la etapa inicial como en mi segunda etapa al retornar a la Universidad.

También a dos excelentes gerentes durante mi etapa en Cargill, quienes compartieron todo el conocimiento y experiencias en función del crecimiento, no solo laboral sino como persona. Ellos son Javier Fantini (IT Business Manager) y Bill Gabby (TGRC Global Manager).

En especial, a mi papá que ya no está, pero seguramente se le dibujará una sonrisa en este momento.

1 INTRODUCCIÓN

1.1 Contextualización

Durante el inicio de la primera década del 2000 el autor del presente informe ingresa al área de Sistemas de la empresa Finexcor; posteriormente la empresa es comprada al finalizar el *due diligence stage*[1] en un 50% por la multinacional Cargill para luego, con el auge de las exportaciones cárnicas durante el primer gobierno de Néstor Kirchner, ser adquirida en su totalidad.

Esta empresa, siempre a la vanguardia en su esfuerzo por lograr ser líder en cada uno de los segmentos que interviene en el mercado internacional, implementa a nivel mundial el programa **TGRC**[2]. El autor integra el grupo *global* de trabajo como responsable para la unidad de negocios del sector en Argentina, reportando directamente al líder mundial Mr Bill Gabby en Mineapolis-US, asumiendo la responsabilidad no solo en todo lo que implica la definición de una política (identificar procesos, evaluación, análisis, etc.), sino también en capacitación de los responsables de sectores en la implementación, evaluación y seguimiento; también integra el equipo de Administración de Incidentes (**ITIL**) como Local Expert para Argentina Beef incluyendo Planta Bernal y Plata Nelson reportando al Sr Anderson Mendes de San Pablo-Br. El complemento de todas estas actividades lo brindaba, para TGRC, la herramienta de software denominada **ARCHER** permitiendo reflejar en ella todos los

[1] En la compra-venta de una empresa es la investigación previa para determinar la situación financiera-empresarial de la misma
[2] Technology Governance Risk and Control

procesos/subprocesos identificados, su valuación, las áreas de riesgo, los procesos críticos, impacto de eventuales "caídas", entre otras tantas funcionalidades. Mientras que para **ITIL** la herramienta de software era **VIATIL Incident**.

Hacer referencia a "global" en una empresa que es líder mundial, significa tener la oportunidad de trabajar, colaborar, asistir y participar de *call meeting* con los referentes y líderes de todas partes del mundo donde la compañía tiene presencia. El autor ha tenido oportunidad de exponer y participar en reuniones cuyos integrantes eran gerentes en Mineapolis, México, Australia, Reino Unido, etc. Las mismas eran semanales donde se exponían los avances y mensuales donde se evaluaban las métricas. Si algo se desviaba demasiado de los objetivos seguramente implicaba una explicación concisa y clara sobre **QUÉ OCURRIO** y **QUÉ PROCESOS o METODOLOGIA IMPLEMENTAR** no solo para alcanzar los objetivos fijados sino también superarlos.

1.2 TGRC como Necesidad o Fundamento del Proyecto

Gobierno, control y seguimiento de los riesgos tecnológicos o **TGRC**, es el término general utilizado para referenciar tres principales áreas: gobierno de riesgos, gestión de riesgos y cumplimiento de las políticas establecidas. Se puede pensar por un instante en la importancia de esta empresa y sus políticas vanguardistas, solo al considerar la publicación de las primeras investigaciones académicas sobre **TGRC** fueron hechas en 2007 al tiempo que el grupo multinacional ya había sido creado y estaba en pleno despliegue de sus actividades. Estas publicaciones mencionaban el tema como *Gobierno y Control de Riesgos,* definiéndola como "colección integrada de capacidades que permiten a una organización lograr objetivos de manera confiable, abordar la incertidumbre y actuar con integridad".

El conjunto de procesos establecidos y ejecutados por los directores reflejan no solo la estructura de la organización sino también como se gestiona para alcanzar los objetivos, situándose en el *gobierno*. Mientras el *control* de los riesgos implica la predicción y gestión de las amenazas que podrían "golpear" la estructura de la organización dificultando el alcance de las metas fijadas, o podríamos decir "alcanzamos los objetivos de manera confiable aún bajo situaciones de incertidumbre".

Toda empresa que pretenda un desarrollo sostenido, con metas medibles y alcanzables deberá implementar **TGRC**, además un control coordinado de sus componentes. Los procesos y actividades superpuestas o duplicadas tienen un impacto negativo en los costos operacionales y las métricas. Si no se integra, si abordamos

tradicionalmente en un enfoque SILO[3], las organizaciones en su mayoría tenderán a poseer un número inmanejable de requisitos relacionados a **TGRC,** debido principalmente a factores tales como los cambios en la tecnología, el aumento de almacenamiento de datos, mayor regulación, incremento de las amenazas tanto externas como internas, la globalización del mercado entre otras que existen y aquellas que surgen semana a semana.

Para ser más estratégico en la gestión de riesgos y el control de sus ambientes, Cargill es capaz de proteger aún más sus clientes y empleados. El soporte en la gestión de las actividades de riesgo se establece en lo que se denomina **Strategic Intent 2015/2020 Goals** (Objetivos Estratégicos Propuestos) incluyendo cómo Cargill es parte y acompaña ese cambio.

1.3 TGRC, Por Qué Necesitamos Gestionar el Riesgo Tecnológico?

Periódicamente podemos escuchar, y de hecho solo al leer un medio internacional encontramos sucesos, nuevos incidentes de seguridad que afectan a diversas compañías. Por lo tanto, la empresa debe gestionar y administrar los riesgos tecnológicos porque el mismo tipo de incidentes puede ocurrir en ella. En la siguiente figura, se puede observar un resumen de riesgos conocidos y procedimientos de control combinados a través de los cuales la empresa enfrenta la situación.

	Ejemplos de Riesgos y Control en la industria		Como mitiga la empresa el Riesgo potencial relacionado
Seguridad de la información	Enero 28,2008. Empresa de ventas francesa sufriría una transacción no autorizada y las computadoras de sus empleados son hackeadas para cubrir el ataque. El costo de esta violación asciende a U$S7.09 billones.	⇨	Un empleado ha terminado pero su acceso a la computadora sigue activo (logueo), después de esto un individuo ingresa y borra datos. Cerca del 100% de las auditorías en el 2009 detectaron el problema de sesiones activas en ausencia del responsable. Entender y gestionar los accesos y la autorización a las principales aplicaciones de negocios debería reducir el riesgo.
	Enero 28, 2007.TJX Companies Inc. (la cual opera TJ Maxx, Marshalls y otros) anuncia que sufrió una instrucción no autorizada en su sistema al proceso de TRANSACCIONES de CLIENTES. El costo de la intrusión fue de U$S216M.	⇨	La empresa usa un Servicio de detección de Intrusiones (IDS) para monitorear los puntos de acceso a internet que la empresa posee. En un mes, se detectaros 1.6 millones de alertas de intrusión, 6 constituían un potencial ataque a la empresa. Entender también que la mayor parte de los ataques en las empresas provienen de empleados desconformes, o sea, interno. Entender y gestionar los accesos y la autorización a las principales aplicaciones de negocios debería reducir el riesgo.
	Dic. 5, 2007. Lo nombres y número de seguro social de 280.000 donantes de sangre almacenados en una laptop que fue robada del Memorial Blood Center en Duluth, Mineapolis, incluyendo varios empleados de Cargill. Incrementando el riesgo de robo de identidad.	⇨	La empresa, en promedio 30-50 laptops son robadas anualmente, más computadoras de escritorio y numerosos dispositivos PDA/USB. La encriptación de los archivos previene los accesos ante un robo o extravío. Una gestión activa de los dispositivos de almacenamiento

[3] Referencia en las organizaciones a su incapacidad para integrar el trabajo en las diferentes áreas o unidades de negocio que la componen

			electrónico que la empresa posee ayuda a reducir el riesgo.
Recuperación de la Tecnología	Las pérdidas financieras por el apagón de 2003 en el nordeste de América del Norte se estimaban en aproximadamente en U$S6 billones. Dos tercios de las empresas entrevistadas posteriormente, manifestaron pérdidas completas del negocio el día del evento. Un cuarto de los negocios encuestados pierden más que U$S50.000 por hs, significa por lo menos U$S400K por las 8 hs del día de trabajo. Y el 4% de los negocios perdieron más que U$S1M por cada hs en que no operaban.	⇨	Una adecuada recuperación de los procesos no ha sido considerada, o aún peor, los procesos no han sido identificados y por lo tanto el nivel de riesgo no definido. Pocas unidades de negocios tienen una prueba completa del Disaster Recovery Plan (Plan de Recuperación de Desastre). La empresa, a 2012, tenía 13 Data Centers y más de 500 almacenes de datos que, durante el trabajo del autor, no habían sido testeados. La empresa pretende desarrollar un Disaster Recovery Plan que reduzca y minimice las pérdidas por fuera de servicio (o corte) permitiendo gestionar de acuerdo al nivel de riesgo del proceso afectado.
Gestión de la Tecnología Activa	Adobe es muy agresivo en su auditoría de software y reconoce que el cumplimiento de las licencias puede incrementar el 10% de sus ingresos. Adobe planea un seguimiento del cumplimiento, ofreciendo la Asociación de Software recompensas por consejos anónimos.	⇨	Anualmente la empresa levanta licencias, tiene a 8.000 instalaciones de Adobe a 2014. Gartner Inc. detectó un promedio del 20% de empresas que no cumplían con la política de la licencia lo que significaría en la empresa aproximadamente U$S4M en multas. La gestión del software activo y su cumplimiento mitigaría el riesgo. Para alcanzar ese objetivo, la empresa realiza auditorías regulares de software activo.

Figura 1. Forma en que mitiga la empresa el riesgo respectivo

1.4 El Abordaje de la Empresa a los Riesgos en la Tecnología

Históricamente, el grupo **CIP**[4] (Protección de la Información-IP) facilita y ejecuta reglas específicas, métodos o actividades para la IP de acuerdo a la unidad específica de negocios (BU[5]) que se trate. Sin embargo, este enfoque no fue efectivo de manera sostenida en la amplia brecha de control que debe efectuar la empresa. Además, en algunas situaciones ciertas BU o Plantas de la empresa esperaban que el grupo IP gestione las cuestiones de seguridad, pero actualmente las mismas son EXCLUSIVA responsabilidad de las BU/Plantas.

Las expectativas que posee el cambio, es en la ejecución de los Controles y Riesgos de la Tecnología entregable. Específicamente, con la organización y roles de **TGRC**, la empresa tiende a:

- Asegurar las ***responsabilidades*** para el control de los riesgos tecnológicos en las BU dentro de los niveles correctos.
- Hacer foco en los ***procesos sostenidos***[6] con un apropiado monitoreo de control.
- ***Ser más estratégico*** en la gestión y administración en los ambientes de riesgo y control. Permitiendo a la empresa una mejor protección de sus

[4] Cargill Information Protection, IP
[5] Business Unit
[6] Sustainable Processes: proceso confiable, replicable y medible sobre resultados confiables

clientes y empleados; ello se refleja en el **Intento de Metas Estratégicas** (SI) alcanzables a 2015/2020 convirtiéndose en *socio del cambio*.

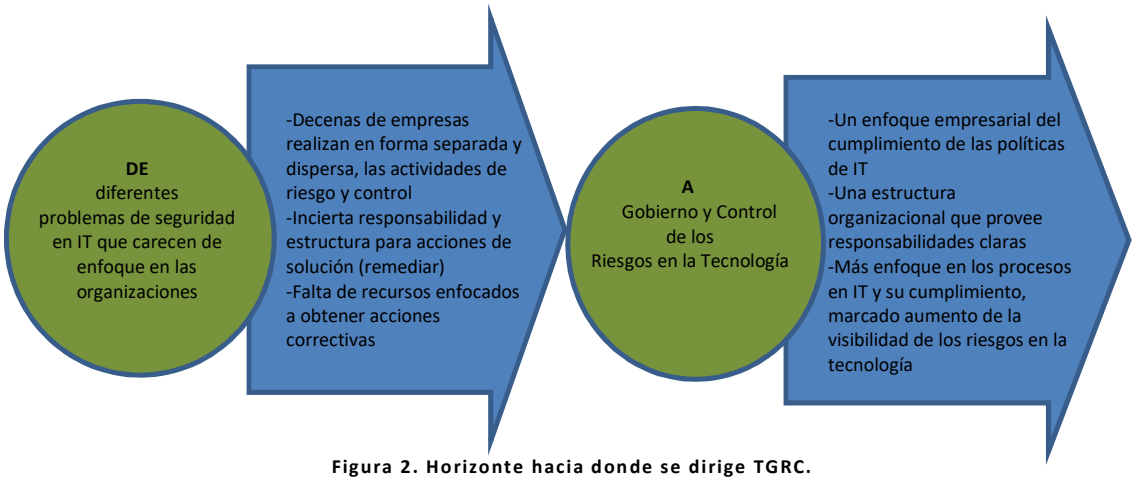


Figura 2. Horizonte hacia donde se dirige TGRC.

1.5 TGRC y su MISION

Sencillamente, la misión de TGRC consiste en:

- Entender las necesidades y conexión que existe entre los socios de negocios y clientes de negocios que la empresa posee a lo largo del mundo.
- Proporcionar liderazgo para los negocios de la empresa en identificar y reducir los aspectos potenciales relacionados a riesgos tecnológicos.
- Permitir a los empleados gestionar-administrar los riesgos tecnológicos y controlarlos a través de una correcta educación, herramientas, y conocimiento, además de compromiso con la empresa.
- Implementar y medir las mejores ideas y soluciones en los riesgos tecnológicos y su control.

1.6 TGRC y su Organización Central en la Empresa de Referencia

La organización central de **TGRC** en la empresa donde el autor tuvo la oportunidad de trabajar, consiste en seis equipos que conducen e integran los esfuerzos para administrar los riesgos y proveer asistencia a los **Risk Managers**, **Risk Analyst**, **IT Managers** y **Controllers** (Gerentes de Riesgos, Analistas de Riesgos, Gerentes de IT y

Controladores respectivamente) a través de las plataformas y el Centro de Servicios Compartidos[7] (SSC). La organización **TGRC** es descripta en mayor detalle enunciando:

- Equipo ***Seguridad en Infraestructura***, administra coordinación y entrega de un amplio monitoreo de la seguridad, administración y gestión de eventos, herramientas y respuesta a incidentes (**ITIL Team**). Es un numeroso equipo en la organización central y para el 2010 incluía también el equipo de **Gestión de la Tecnología Activa**[8]. Este grupo establece y mantiene una amplia variedad de políticas y estándares que refieren a tecnología activa en la empresa, además de proveer guías y herramientas para implementación que deben ser SIEMPRE satisfechas, incluyendo administración de derechos[9] sobre Hardware, Software y equipos de utilidad electrónica.
- Equipo ***Proveedor de Servicio Externo***[10] (OSP) establece y audita el conformidad de las conexiones de los terceros conectados a la empresa, al igual que aquellos proveedores de servicios críticos. El equipo OSP también coordina la regulación de los requerimientos tecnológicos y comunicar estos a las Plataformas/SSCs.
- Equipo de ***Políticas y Conocimiento***[11] sirve como un recurso proporcionando colaboración y servicio de consultas con las Plataformas/SSCs, siendo soporte en el desarrollo y entrega (puesta a disposición) de los conocimientos relacionados a los riesgos incluyendo programas de entrenamiento.
- Equipo de ***Programas y Controles***, proporciona liderazgo, entrega de software, administración de proyectos y gestión de los recursos relacionados a riesgos tecnológicos en la empresa. Este equipo lidera el Comité de la Administración del Riesgo Tecnológico, es responsable de la gestión y el reporte de las mediciones de la empresa en **TGRC** y representa a **TGRC** como una línea de negocio. El equipo también incluye los Gerentes y Analistas de región (el autor trabajó en LA[12] Beef) quienes son responsable del liderazgo y soporte regional.
- Equipo de ***Gestión/Administración de las Contingencias***[13], establece y mantiene una amplia variedad de políticas y estándares aplicables a situaciones de contingencias, incluso proveer herramientas y guías para su implementación, que incluyen:
    - ***Análisis de Impacto de Negocio***(Business Impact Analysis - BIA)

[7] Shared Service Center
[8] Technology Asset Management
[9] Copyrights
[10] Outside Service Provider
[11] Policy and Awareness
[12] Latin America
[13] Resiliency Management

- ***Plan de Continuidad del Negocio*** (Business Continuity Plan - BCP)
- ***Administración de Crisis*** (Crisis Management - CM)
- ***Plan de Recuperación de Desastre*** (Disaster Recovery Plan – DRP)

Este equipo también lidera el Comité de Administración de Crisis y donde el autor desarrolló el completo plan Resiliency Management para Beef Argentina.

- Equipo de ***Seguridad de las Aplicaciones***[14], administra los procesos, estándares, herramientas y metodología usada para asegurar que el software es desarrollado de manera segura a los intereses y políticas de la empresa. También trabaja con la Plataforma/SSC para asegurar que el software puede ser usado de manera confiable, no es vulnerable a los ataques y su riesgo ha sido identificado/mitigado.

1.7 TGRC y su Plataforma

La organización **TGRC** despliega cada Plataforma y SSC a cada región geográfica.

Un gerente de TR&C[15] en cada Plataforma y SSC reporta al **TGRC** líder. En el caso particular del autor, el gerente de Sistemas de Beef Argentina era el Sr Javier Fantini desplegando las funciones de gerente de Plataforma y SSC, en tanto Mr Bill William Gabby era el líder Global. En la mayoría de las Plataformas y SSCs, hay también uno o más Analistas de Riesgos Tecnológicos reportando a el TRCM[16], además, hay un TRCM en cada región fuera de Estados Unidos en donde cada gerente y su analista trabaja estrechamente con el líder global para asegurar que los requerimientos considerados son satisfechos. Por este diseño de las Plataformas, ***el autor del presente proyecto trabajaba muy estrechamente con el Sr J. Fantini y Mr Bill Gabby en todas las funciones del grupo TGRC para Beef Argentina***. *Otros equipos en el mundo de similares características al del autor (tipo de Unidad de Negocios, cantidad de personas, modo de trabajo, etc.), también reportaban al líder global y formaban parte de equipo de Programa y Control en la organización* ***TGRC*** *Central*.

Es importante resaltar esto último, puesto que al hacer referencia al rol de TGRC Central Organization, se estará haciendo referencia directa al rol del autor y su correspondencia en cuanto a las actividades desplegadas.

[14] Application Security
[15 Technology Risk and Control
[16] Technology Risk and Control Manager

En el siguiente cuadro se puede apreciar la Plataforma Global del grupo de trabajo para el Gobierno y Control de Riesgos Tecnológicos:

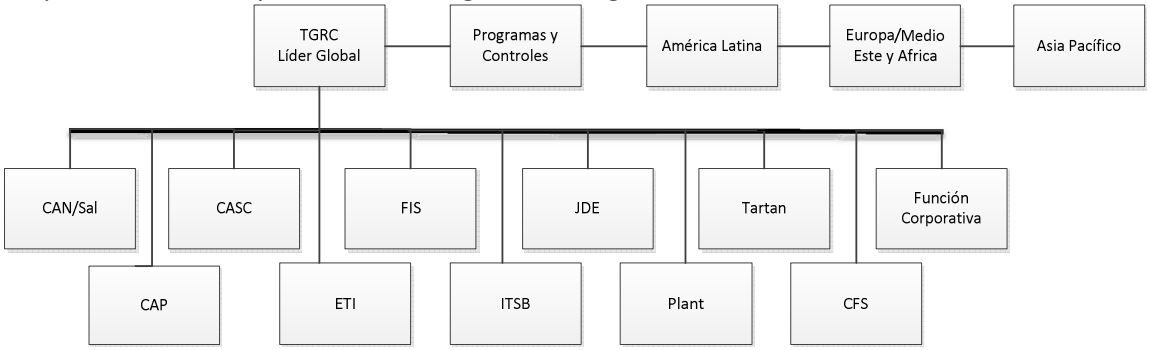


Figura 3. Plataforma Global de TGRC

1.8 Resumen de Roles

Empresa

- Desarrollo de entrenamiento (conocimiento, usuario final, etc.)
- Desarrollo de comunicación (traducción cuando es necesario)
- Estandarizar procesos para conectividad de terceros
- Verificar cuando una oficina legal regional aplica las políticas de IP
- Seguimiento de los planes acción de validación y otras iniciativas de conformidad
- Reportes de medición para métricas definidas en la empresa
- Establecer relaciones con las partes interesadas como factor clave
- Establecer herramientas y procesos SAM(Software Asset Management)

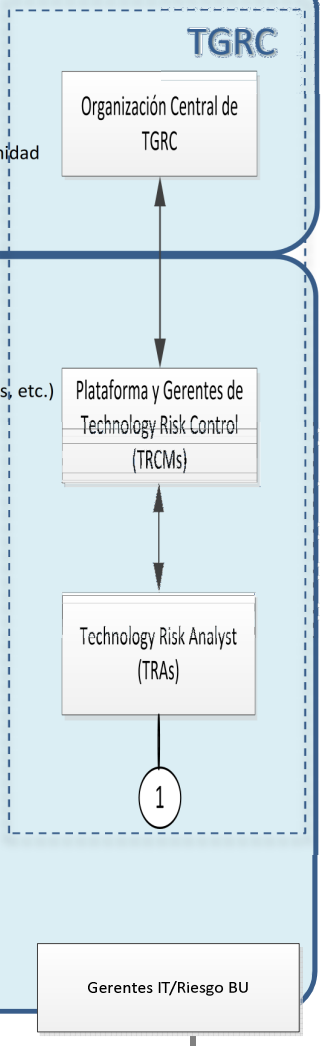
Plataforma/SSC

TRCMs

- Asesor de riesgo en la BU correspondiente para eliminar o reducir el mismo
- Responsable del programa TRC en la Plataforma/SSC
- Proveer liderazgo para las iniciativas de TGRC (auditorías semanales, informes, etc.)
- Proveer liderazgo y guías a los TRAs, BRMs y SRCC[17]
- Revisar y aprobar la variación de IP y acción de aceptación de riesgo
- Proveer liderazgo y guía a los Analistas de Riesgo e implementadores de soluciones aconsejables

TRAs

- Son el soporte para la validación de los procesos de auditoría y las acciones correctivas (supervisión en sitio, reportes, seguimiento, etc.)
- Comunicar y entrenar (generar conocimiento, control seguridad IP, inducir conciencia, Controlar, etc.)
- Consultoría (escalabilidad para clasificación de políticas, seguimiento de auditorías)
- Monitoreo (asegurando *walkthrough*, inducir al buen comportamiento y todas aquellas actividades de TGRC necesarias en el sitio)
- Validar y monitorear la gestión del software activo en acuerdo a las prácticas Aconsejadas (SecurCompass) en la Plataforma/SSC
- Elaborar en forma completa y detallada el Resiliency Management Plan intentando abordar la mayor parte de los riesgos (BIA, BCP, DRP y definir CMC[18])



[17] Technology Risk Analyst, Business Risk Manager y Site Risk Control Coordinator
[18] Crisis Management Committee

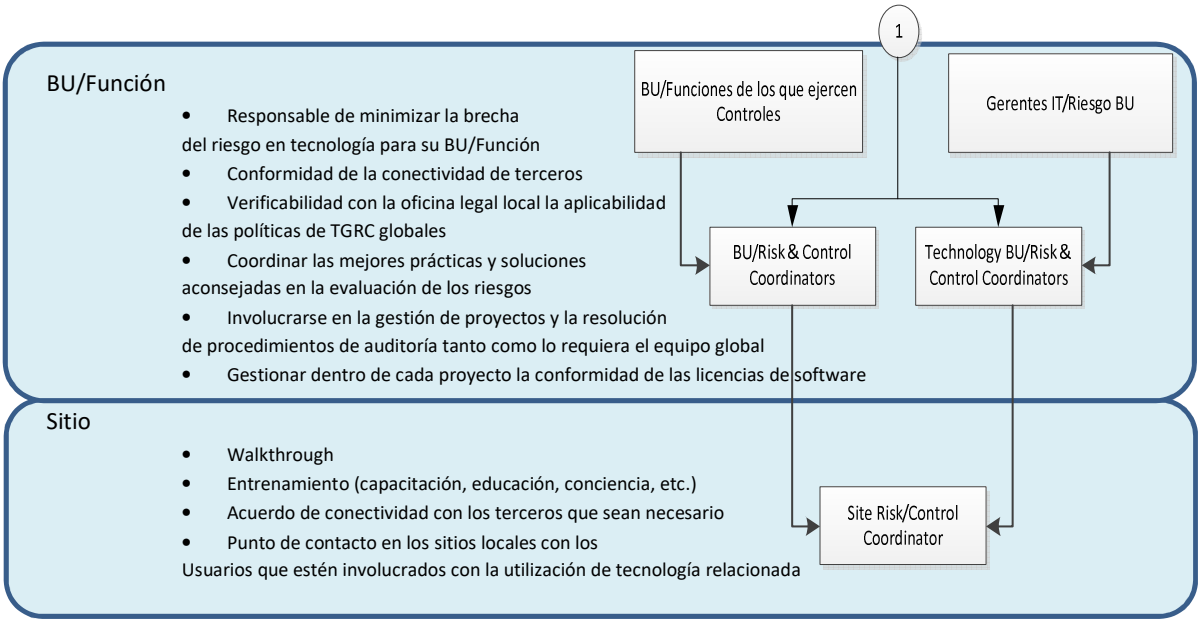


Figura 4. Resumen de Roles del autor, con excepción de los que poseen rango de *Manager donde compartía funciones con Javier Fantini (IT Manager para Beef Argentina) en lo que respecta a TGRC.*

El gráfico anterior provee un resumen de varios roles en **TGRC**, describiendo algunas de las responsabilidades o alcances relacionados con cada rol. ***La lista de roles incluye al Technology Risk and Control Manager (TRCM para el caso del autor lo asumía el Sr Javier Fantini), Technology Risk Analyst (TRA, en el caso del autor asumía estas responsabilidades), Technology Risk Control Coordinator (TRCC, al asumir el autor la responsabilidad para las dos plantas pertenecientes al Beef BU, estas funciones son incorporadas), BU o Function Risk Control Coordinator (RCC) y Site Risk Control Coordinator; estas últimas también responsabilidades asumidas por el autor trabajando en ambas plantas (Bernal y Nelson).***

1.9 TGCR, Mapa de Despliegue

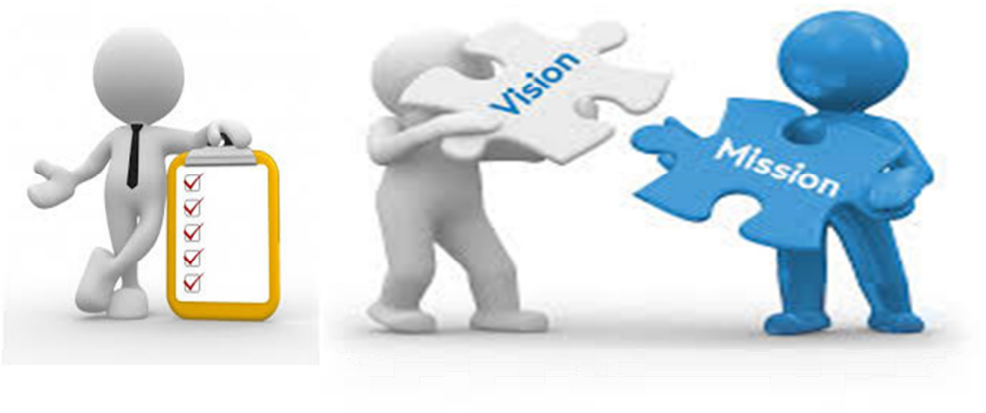
La organización **TGRC** estaba planeada, y de hecho implementada, para aplicar numerosas iniciativas tendientes a reducir el riesgo de exposición de la compañía a los ataques, teniendo en cuenta que los mismos podían provenir tanto del exterior como ser internos; ***de nada serviría el firewall más sofisticado, la política de software más completa, el proxy más restrictivo, las mejores configuraciones de las iptables de ruteo si se ha olvidado deshabilitar por ejemplo un USB y un empleado desconforme introduce un pendrive apropiándose de información susceptible o desplegando un virus***.

INICIATIVA	DESCRIPCION
Privacidad de los datos	Desarrollar un amplio, profundo y agresivo plan de privacidad en todas las líneas y niveles de la empresa. Obtener la aprobación del Programa de Privacidad de la Autoridad Nacional Supervisora, implementar práctica de privacidad de los datos, establecer una implementación de respuestas a incidentes y abrir un procedimiento o proceso para aquellas faltas de incumplimiento en las mismas.
Seguridad en el Software	Implementar el análisis del código fuente por personal idóneo y definir las herramientas necesarias para detectar y prevenir problemas de seguridad en aplicaciones, además de acompañar con un entrenamiento activo.
Análisis de Impacto de Negocio - BIA	Implementar un plan consistente basado en la aplicación web Archer para lograr un abordaje de la propuesta a lo largo de toda la compañía. Usar Archer para almacenar los planes de Recuperación de Desastres (DR) y BIA o monitorizar el avance y cumplimentación de los mismos, al igual que su correspondiente prueba. Archer será una aplicación que merece un capítulo.
Prevención de pérdida de datos	Implementar un software monitor altamente securizado y bloquear todos los emails salientes de la empresa que posean contenido inapropiado tal como número de seguro social, números de cuentas bancarias o información confidencial. Ciertos patrones detectados en los emails, posibilitaba el procedimiento.
Gestión de Crisis	Mejorar sustancialmente la habilidad de la empresa en los procedimientos y métodos usados para comunicar la información durante una crisis, además de gestionar correctamente la respuesta de la parte de interés. Información clara, concisa, correcta y en el tiempo apropiado es fundamental durante una crisis.
Mejoras en Archer	Mejorar el software de aplicación Archer mediante su correcta configuración y modificación en las capacidades de la herramienta.
Clasificación de la Información	El estándar de la clasificación de la información debe ser actualizado para los nuevos controles y requerimientos que surgen como consecuencia de la implementación de nuevos procesos, nuevas políticas, nuevas tecnologías, nuevas amenazas, etc.
Gestión de los Servicios Provistos Externamente - OSP	Implementar nuevos métodos, basados en Archer, de administración o gestión OSPs a través de un seguimiento centralizado de las empresas, automatizar cuestionarios, definir las recomendaciones y planes de acción para corregir diferencias o deficiencias.

Tabla 1. Despliegue propuesto por TGRC a nivel mundial.

Los programas, procesos o metodología listados arriba son ejemplos de las iniciativas del equipo **TGRC**. Los ejemplos corresponden a modificaciones que tendrán en termino de impacto, un nivel de considerado alto a medio en la unidad de negocios (BU).

Como avance en la planificación, ejecución y seguimiento del proyecto implementado por **TGRC**, las áreas o departamentos RCCs, TRCCs y SRCCs serán informadas de cada iniciativa que las involucre o afecte, al igual que el papel o rol que tendrá este nuevo riesgo -si es que lo hubiera- en el esfuerzo por la gestión y administración de las amenazas.



2 POLITICAS DE TGRC, MISION DE LA EMPRESA Y PLAZOS DEL PROYECTO

2.1 Políticas y su Alcance

Antes de definir el alcance de las políticas de la empresa en general y específicamente referidas a **TGRC**, el autor estima conveniente hacer una breve definición y diferenciación entre políticas de negocio y procesos de negocio.

Una política es un conjunto de principios y directrices relacionadas que una empresa establece para definir sus objetivos a horizonte lejano, dirigir y limitar el alcance de sus acciones en la búsqueda de sus metas a largo plazo y proteger sus intereses.

Ahora bien, un procedimiento es una manera de completar una tarea para obtener una salida esperada, consiste en una secuencia de pasos o curso de acción (con punto de inicio y fin perfectamente establecidos) que deben ser seguidos en el orden definido para completar correctamente una tarea. Procedimientos repetitivos son denominados rutinas también llamados métodos.

Entonces, políticas son declaraciones amplias adoptadas por el negocio o empresa estableciendo que significa el negocio y cuáles son sus objetivos. Mientras los procedimientos son usualmente implementados para respaldar cada política desplegada que explica en su esencia como aplicar la política a los empleados, clientes, proveedores y productos de la empresa, alcanzando también a los métodos de producción; por lo tanto, estas “instrucciones” son necesarias para llevar adelante la implementación de las políticas. Ejemplos de *dónde* la empresa o unidad de negocio

establecen políticas, además de **TGRC**, son ética, recursos humanos, contaduría y servicios al cliente entre otras tantas áreas. La combinación de políticas-procedimientos tendrán más importancia cuanto más ambiciosa sea la misión y/u objetivos de la empresa a un determinado plazo.

2.2 Declaración General de Políticas sobre la Información

Los miembros de la comunidad[19] de la empresa, incluyendo empleados, clientes y proveedores, confían en la tecnología en múltiples aspectos de su trabajo, negocios, conocimientos, desarrollo y tantas otras actividades para desarrollar su tarea. Al hacerlo, utilizan sistemas electrónicos y redes (solo por citar algunos) que la empresa posee, proporciona y administra; poniéndolos a disposición con el fin de poder llevar adelante las actividades. Para promover la confianza dentro de la comunidad, la empresa debe ser trasparente sobre las políticas con respecto a las circunstancias en las que puede acceder la información electrónica del usuario almacenada, transmitida a través de estos sistemas o divulgada fuera.

El compromiso de cumplimiento de las políticas establecidas no es suficiente, además se necesita una expresa conformidad a través de lo denominado como CONTRATO DE CONFIDENCIALIDAD. El mismo es de estricto cumplimiento y sancionable legal u organizacionalmente ante una falta. El autor del presente proyecto, para poder realizarlo, ha debido solicitar autorización a Mr Bill Gabby quien como responsable mundial del grupo **TGRC**, aceptó tomando ciertos recaudos o mencionando algunas aclaraciones sobre los derechos o imágenes.

La política de la organización se basa en seis principios importantes:

- El acceso debería ocurrir solo a propósitos específicos e importantes de la empresa.

- El acceso debería ser autorizado por la persona apropiada y responsable.

- En general, se debe ser capaz de mantener tanto un registro o informe de las personas que acceden y utilizan la información como también que aplicaciones, archivos o recursos tiene un hardware propiedad de la empresa.

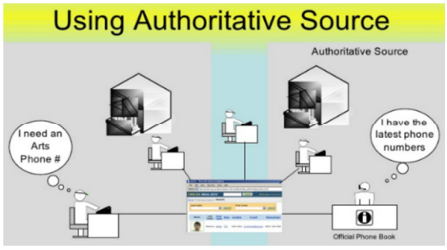
[19] Comunidad: empleados, proveedores, clientes y medio ambiente en un radio de 60km a una BU

- Los accesos deben ser limitados a los recursos tecnológicos de la compañía, con el principio de brindar solo lo necesario para realizar el trabajo, función o procedimiento que el usuario-empleado debe efectuar. Vale la pena esta aclaración, porque en ciertas situaciones el usuario es un tercero (proveedor o cliente).
- Los registros de acceso se deben mantener en forma apropiada y centralizada para poder realizar un seguimiento de las políticas definidas.
- El acceso a los recursos o información debe estar sujeto a la revisión continua e independiente (no pertenecer a la BU), en el caso de la empresa en cuestión el acceso era revisado por un grupo de **TGRC**.

2.3 TGRC, Centro de Terminología de Política

Políticas y Áreas. Las políticas definen la gestión en administración y las guías para implementar la seguridad IT en las actividades específicas. Área, formalmente conocido como *estándares*, corresponden a segundo nivel más alto en el marco de políticas describiendo propósito y ámbito de las normas de control subyacentes.

Estándares de Control. Los estándares de control, formalmente conocidos como *objetivos*, especifican el curso de acción o respuesta a dar a una determinada situación. Los estándares de controles son directivas obligatorias para llevar adelante la gestión de las políticas y son usadas para medir su conformidad, es decir, el modo en que se ajustan a las mismas. Los estándares sirven como especificación para la implementación de las políticas corporativas.



Fuentes Autorizadas. Incluyen interna, legislativa, externa, requerimiento de mejores prácticas que en una organización deben reunirse o alinearse con los riesgos medibles, demostrar conformidad y posicionarse junto a los objetivos

planteados, propuestos y delineados por la empresa.

Procedimientos de Control. Incluyen paso por paso los procedimientos para documentar las actividades de control y tareas para los procesos de negocios y las tecnologías usadas. También proveen revisión de evaluación para los procedimientos de auditoría que pueden ser usados para los controles de validación.

El Centro de Terminología Política funcionaría como un repositorio general y mundial donde se establecen y almacenan los estándares adecuados para asegurar la calidad e integridad de la información de la empresa.

Frente a la importante cantidad de procesos, información y recursos; el almacenamiento centralizado de todas las políticas suele ser una fuente de consulta para los empleados a nivel mundial que posean acceso.

El conjunto de conceptos utilizados como pilares de la implementación de los más altos estándares utilizados por **TGRC** para lograr la certificación internacional, estaban compuesto entonces por: Políticas y Áreas, Estándares de Control, Fuentes Autorizadas y Procedimientos de Control.

Conceptos que una vez definidos y almacenados, estaban en continua actualización para *aggiornarse* a la vertiginosidad de los cambios.

En la Unidad de Negocios Beef Argentina, el autor efectuó un importante trabajo al ser una BU adquirida e incorporada en total funcionamiento. Implicando la completa definición antes mencionada.

Marco base de políticas Cargill Technology Governance Risk & Control

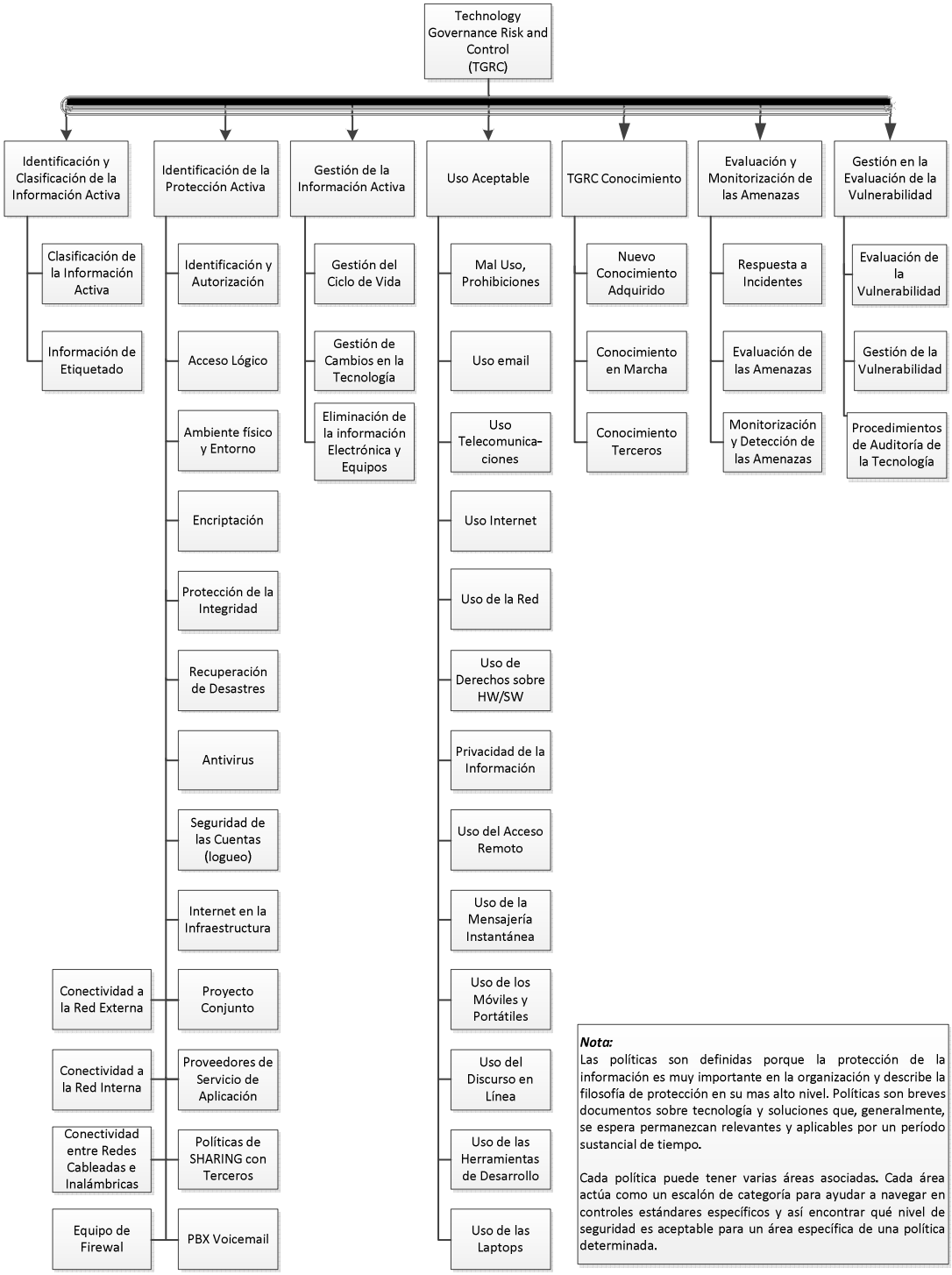


Figura 5. Marco del conjunto de políticas bases.

2.4 Dónde son Almacenadas las Políticas?

Las políticas y sus diferentes áreas, si es que poseen varias, son almacenadas en una herramienta web denominada **Archer**.

Es una herramienta de una navegación muy simple y amigable. A través de ella se navega en una multitud de políticas y áreas usadas para describir el Mapa de Políticas. Cada cuadro que posee la URL, es coloreado de manera apropiada para referenciar aún más la política o el área.

La siguiente imagen sirven para contextualizar al lector sobre la estructura de la aplicación, cuyo desarrollo el autor lo brindará posteriormente mereciendo un capítulo especial.

La importancia de esta herramienta era tal en la empresa que una carga errónea en la definición de un proceso, implicaba recibir un email con invitación a una reunión telefónica con los líderes, la misma era de carácter obligatoria, sin posibilidad de rechazo y con hora establecida en base al uso horario manejado por Mineapolis. Surge entonces otra implicancia: la calificación de HIGH a todo lo que era identificación de procesos, subprocesos y actividades que componían la Unidad de Negocios, abarcando para el caso del autor Beef Bernal Unit (FINEXCOR Bs. As.) y Beef Nelson Unit (FINEXCOR Sta. Fe).

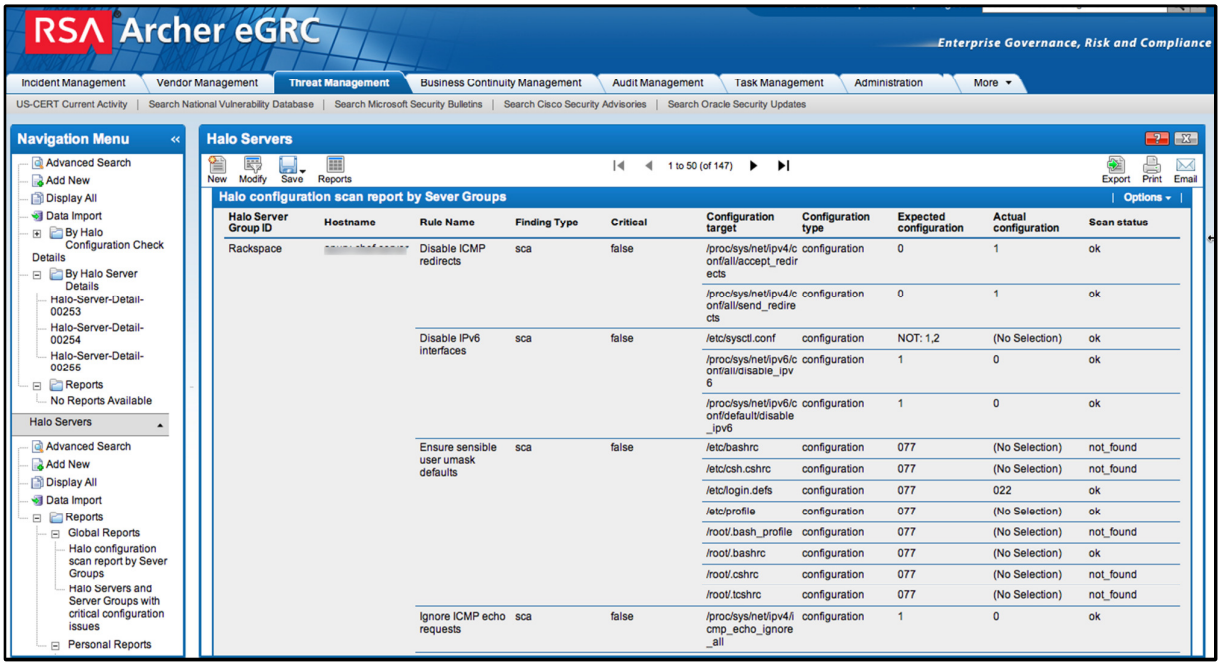


Figura 6. Archer, Gestión de Amenazas.

2.5 Misión, Visión y Principios Guías

La misión y la visión se relacionan, ambos, con el propósito de una organización y son generalmente comunicados por escrito. Siendo conceptos que brindan una declaración dentro de la empresa respondiendo a preguntas tales como **quienes somos**, **que valoramos** y **hacia donde vamos**. Una correcta declaración de misión comunicará la razón de ser de la organización tanto a empleados, clientes y proveedores como a la propia comunidad donde la empresa se sitúa, incluyendo además, cómo pretende servir a sus partes interesadas. Los clientes, empleados e inversores son las partes que se destacan con más frecuencia, pero también se suele incluir otros, como por ejemplo el gobierno y la comunidad (es decir su impacto social y ambiental). Una correcta definición de una misión deberá mencionar una suma de valores de la empresa.

Una declaración de visión, en cambio, es una declaración orientada a futuro sobre el propósito y las aspiraciones. En este sentido, se podrá observar la declaración de la misión establece "el propósito de ser" de una organización, y la declaración de visión suele incorporar terminología tal como "en función de ese propósito, esto es lo que queremos llegar a ser. Le estrategia debería fluir directamente de la visión, ya que la estrategia está destinada a lograr la visión y así satisfacer la misión de la empresa.

En la empresa de referencia, la misión se basa en la filosofía de nutrir a las comunidades en las que opera, enfocando su estrategia de responsabilidad social empresarial en el bienestar de las comunidades donde opera. Así, poder transformarse en un socio en el que es posible confiar para prosperar, hoy y en el futuro, manteniéndose al día con los mercados que cambian rápidamente y los gustos de los consumidores. La visión es crear valor para todos en cada oportunidad.

La visión en desde la perspectiva de la empresa:

Al 2020, seremos reconocidos como una empresa líder en impacto social en materia de nutrición y educación en las comunidades donde operamos y por contribuir con el desarrollo de nuestra gente, clientes y proveedores permitiéndoles prosperar.

Los principios guías, entre otros, se detallan a continuación:

- Respetar la ley y conducir el negocio con integridad
- Mantener registros precisos y honestos
- Honrar las obligaciones comerciales
- Proteger la información, los activos y los intereses de la empresa

Piense el lector por un momento lo que serían estos objetivos realmente ambiciosos sin un conjunto de políticas, vistas anteriormente, en las cuales soportar y regular el comportamiento tanto de clientes, empleados, proveedores y terceros… sería la nada misma. Por este motivo, **TGRC** es un componente fundamental en la búsqueda de las metas propuestas, tres de los cuatros principios guías expuestos anteriormente involucran al equipo **TGRC**.

En la actualidad la información electrónica y su protección adquiere, tal vez, importancia nunca antes observada.

2.6 Plazos de Ejecución

Para 2012, Cargill se consolidaba como un proveedor internacional de productos y servicios de gestión de alimentos, agricultura y riesgos, estaba listo para grandes cambios. Ya líder del mercado con 159.000 empleados y $ 116 mil millones de dólares en ingresos, Cargill estaba dando un paso audaz y bien planificado para lograr sus objetivos estratégicos y aspiraciones de crecimiento. A través de **Tartan**, Cargill conectará 80 unidades de negocios en 70 países bajo un proceso de negocios común y un modelo de gobierno habilitado por SAP y otras tecnologías. En su discurso en la Universidad de Minnesota, John Geisler, vicepresidente corporativo y Líder de **Tartan**, destaca las lecciones aprendidas después de los primeros dos años de este viaje de una década y cómo Cargill sostendrá este cambio. En estos años estaba muy involucrado en el proyecto **Tartan**, que es una empresa corporativa importante para mejorar y rediseñar los procesos comerciales clave que se utilizan para administrar y gestionar los negocios y hacerlos comunes en Cargill. También es para mejorar la forma en que captura y mantiene la información comercial crítica, la estandarización de los datos clave de Cargill, así como para simplificar y consolidar la cartera de aplicaciones de software, y actualizar la tecnología que los soporta para tener la infraestructura adecuada para respaldar los negocios de la empresa como metas u objetivos a 2015/2020.

Como parte del Proyecto **Tartan**, el autor fue responsable de la Unidad de Negocios Beef Argentina en lo que respecta a todo lo descripto en el presente trabajo. Desarrollando principalmente funciones en identificación de procesos, áreas involucradas, seguridad informática, parches de antivirus en laptops-desktop-server, plan de contingencias, plan de recuperación de negocios, auditoría de usuarios, administración de cuentas Active-Directory, JD Edwars y Unix, walkthrough, entre otras responsabilidades.

En la siguiente tabla se puede apreciar uno de los componentes observados y evaluados mensualmente:

Elemento Evaluado	Rango de Calificación		
Business Impact Analysis	< 80%	80%-90%	> 90%
Disaster Recovery	< 80%	80%-90%	> 90%

Tabla 2. Calificación utilizada.

A pesar de ser un proyecto autogestionado, es decir, se podía administrar el tiempo dedicado en la realización de las etapas; había que exponer avances en las reuniones telefónicas semanales en conjunto con los demás responsables de las otras unidades de negocios en el mundo.

Tartan debía tener una conformidad cercana al 100% para el final del año 2012.

3 MÉTRICAS

3.1 Qué son las Métricas?

Gestionar un proyecto exitoso significa mantenerse al tanto del progreso. Pero… ¿qué significa eso realmente?

Cada vez más, el éxito se mide por los datos, generalmente el producto final de objetivos y métricas claramente definidos. El auge de Internet de las cosas y Big Data significa un énfasis creciente en el análisis para medir el progreso y el rendimiento, también conocidas como **Visualizaciones de Datos**.

Cada proyecto desplegado en una organización, está inundado de datos cuantificables que pueden usarse para seguir el estado del proyecto, su rendimiento y, en última instancia, su éxito. Obviamente, las partes interesadas quieren que se les muestre exactamente cómo va su proyecto.

Las métricas usadas, principalmente en los proyectos de ingeniería, son medidas cuantitativas que permiten a los administradores evaluar el estado de un proyecto en curso, rastrear riesgos potenciales, descubrir áreas potenciales antes de que sean críticas, ajustar el flujo de trabajo y evaluar la capacidad del equipo de proyecto para controlar calidad de las implementaciones a largo plazo.

Constituyéndose en una valiosa herramienta de gestión en los procesos y proyectos que lleva adelante una organización durante, generalmente, largos períodos de tiempo proporcionando un conjunto de indicadores que permitan detectar desviaciones y delinear mejoras.

Technology Governance Risk and Control Plan es un proyecto donde las métricas se erigen como un factor indispensable para gestión a nivel global.

3.2 Necesidad de Métricas

Considere esto: la mayoría de las corporaciones buscan maximizar el valor de sus acciones a largo plazo. En términos prácticos, esto significa que cada dólar invertido por una empresa debería generar más de un dólar de valor. ¿Qué estadísticas, entonces, deberían usar los ejecutivos para guiarlos en esta creación de valor? Como hemos notado, EPS[20] es el más popular. Una encuesta de compensación ejecutiva realizada por Frederic W. Cook & Company descubrió que es la medida más popular del desempeño corporativo, utilizada por casi la mitad de todas las empresas. Los investigadores de la Stanford Graduate School of Business llegaron a la misma conclusión. Y una encuesta de 400 ejecutivos financieros realizada por los profesores de finanzas John Graham, Campbell Harvey y Shiva Rajgopal encontró que casi dos tercios de las empresas colocaron EPS por primera vez en un ranking de las medidas de desempeño más importantes reportadas a los de afuera. Los ingresos por ventas y el crecimiento de las ventas también obtuvieron una alta calificación para medir el desempeño y comunicarse externamente.

Por supuesto, las empresas también usan medidas de desempeño no financieras, como la calidad del producto, la seguridad en el lugar de trabajo, la lealtad del cliente, la satisfacción de los empleados y la voluntad del proveedor de promocionar un producto. En su artículo de Harvard Business Review de 2010, los profesores de contabilidad Christopher Ittner y David Larcker escribieron que "la mayoría de las empresas han hecho pocos intentos por identificar áreas de desempeño no financiero que podrían avanzar en su estrategia elegida. Tampoco han demostrado un vínculo de causa y efecto entre las mejoras en esas áreas no financieras y en el flujo de efectivo, el beneficio o el precio de las acciones". La encuesta de 157 compañías mostró que solo el 23% había realizado una modelación exhaustiva para determinar las causas de los efectos que estaban midiendo. Los investigadores sugieren que al menos el 70% de las empresas que encuestaron no consideraron la persistencia de una medida no financiera o su valor predictivo. Casi una década más tarde, la mayoría de las empresas aún no logran vincular causa y efecto en su elección de estadísticas no financieras.

[20] Earning Per Share: Ganancia Por Acción

Nuevamente marcando tendencias como empresa líder en el mundo, Cargill, implementa el Proyecto **Technology Governance Risk & Control,** incluido dentro del **Proyecto Global Tartan,** incorporando un conjunto de métricas a nivel mundial.

En la medida u orden que se pretende una gestión eficiente de los riesgos tecnológicos, debemos ser capaz de medir o evaluar nuestra seguridad para poder mitigar aquellos riesgos que podrían golpear nuestra organización. Debemos comprender que el *tablero de control*[21], utilizado en la medición, no captura todos los riesgos en la tecnología activa dentro de la organización. Aun así, es considerado un buen indicador dentro de la empresa hacia la securización de la tecnología.

3.3 Tablero de Control o Scorecard

Seis áreas son medidas con la utilización del *scorecard* de **TGRC**, ellas son:

- Conformidad o cumplimiento de los planes **Recuperación de Desastres** y **Análisis de Impacto de Negocio** (DR y BIA).
- Conformidad de los **accesos** lógicos y reales a la información.
- Gestión de **Procedimientos** de Auditoría.
- Conformidad de **Antivirus**.
- Conformidad en **Parches** de Seguridad.

Los puntajes o calificaciones son calculados por la Plataforma o Centro de Servicios Compartidos (Platform/SSC), aun así, la habilidad para profundizar en algunos aspectos o áreas de las métricas es facultad pura y exclusiva de la Unidad de Negocios o Función específica.

El *scorecard* se alinea detrás de las exigencias de la oficina del CEO[22] en la determinación de las Principales Áreas de Riesgo para los cuales toda la Plataforma y Centro de Servicios Compartidos se moverá a lograr “verde” en el ranking a cierre del año fiscal (principio de julio de un año a fin de junio del siguiente). En el caso del trabajo desarrollado en Cargill por el autor, el último año fiscal fue 2012-2013.

Un aspecto importante a resaltar, el *scorecard* puede -en sí mismo- cambiar y los parámetros medidos o identificados como “observables” pueden alterarse en cada año fiscal. Al tiempo que nuevos riesgos pueden ser identificados lo que ocasionará modificaciones en el *scorecard* al incluir medidas que ayuden a mitigar aquellos nuevos riesgos.

3.4 Elaboración del Tablero de Control o Scorecard

[21] Scorecard
[22] Chief Executive Officer

Las dos aplicaciones principales con las que se llevaba adelante el Proyecto **TGRC** eran:

- Altiris Software Agent/Server
- Archer Tool

Archer Tool se dejará para el siguiente capítulo.

Altiris Software Agent es un software de Symantec, instalado en las computadoras de los usuarios de la compañía, mientras que ***Altiris Software Server*** es la versión de ese software corriendo en el servidor. El software agente instalado en las computadoras que desea administrar facilita las interacciones entre ***Notification Server*** y una computadora administrada. El agente recibe solicitudes de información de ***Notification Server***, envía datos a ***Notification Server*** y descarga archivos. ***Altiris Agent*** también le permite instalar y administrar complementos de solución que agregan funcionalidad al agente.

Altiris Agent permite a los usuarios transmitir automáticamente las aplicaciones. La primera vez que un usuario accede a una aplicación de transmisión, ***Altiris SVS*** instala automáticamente ***Altiris Agent***. El agente ***Altiris*** contiene el administrador de aplicaciones.

Continuamente el agente está levantando datos y almacenando información del usuario y mensualmente enviando los mismos al servidor. La automatización de estos movimientos eran responsabilidad de cada encargado de **TGRC** para la Unidad de Negocios determinada, asumiendo el compromiso de no compensar la ejecución de las políticas con ***performance*** o rendimiento. Eligiendo así la forma y el tiempo más conveniente para cualquier tarea o actividad que consuma ancho de banda o genere gran flujo de datos.

Ello implicaba un análisis de los centros de trabajo, su tiempo de residencia en CPU, tiempo de procesamiento, velocidad de los puntos de acceso, ancho de banda dentro y fuera de la organización solo por citar algunos. El análisis minucioso del comportamiento o desempeño del sistema implicaba parámetros de medición para tener una estimación de cómo un software utiliza un hardware bajo determinadas situaciones de carga, lo que consecuentemente llevaba a una correcta y óptima configuración de los principales componentes del software. En definitiva, la empresa como la gran mayoría, utiliza una arquitectura de ***Sistemas Distribuidos*** donde los componentes se comunican y coordinan mediante el intercambio de mensajes.

3.5 Ejemplo de Datos del Scorecard o Tablero de Control

A continuación, se muestran diferente información incluida en el *scorecard* o tablero de control, la misma se encuentra en formato original para que el lector pueda tomar dimensión de los controles en avances exigidos desde Estados Unidos.

En septiembre de ese período, el autor anexa a sus funciones la tarea de control de parches en la unidad de negocios Beef Argentina, abarcando Planta Bernal y Planta Nelson, obteniendo importantes resultados reconocidos desde Estados Unidos, los que para el último mes anterior al traspaso de la compañía a manos de Fiar S.A. se posicionó como una de las mejores Unidades de Negocios de la compañía en el mundo.

TGRC Metrics	Report Period: March 2011	CANAPS	
Areas of Focus		Actual	Trend
	# of Applications in Inventory	354	
	% of Measures Answered	86%	↓
Business Impact Analysis			
	Application-based BIA Completion Average	99%	
	Application-based BIA Completed	100%	
	Application-based BIA Updated or Created in the Last Year	98%	
	Process-based BIA Completion Average	27%	↑
	Policy-based BIA Completed	32%	↑
	Policy-based BIA Updated or Created in the Last Year	22%	↑
Disaster Recovery		95%	↑
	DR Requirements - # of Applications	40	↓
	Has DR Plan	98%	→
	DR Plan Implemented	98%	→
	DR Plan Tested	95%	→
	DR Test Conducted in the Last Year	88%	↑
Information Access Controls		90%	↑
	Doc. Proc. For User Administration	95%	→
	Doc. Proc. For Approving Access Requests	98%	→
	Doc. Proc. For Immediate Removal	98%	→
	Doc. Proc. For Access Change Notification	98%	→
	Doc. Proc. For Monitoring	98%	→
	Doc. Proc. For User Access Reviews Every 12 Months	99%	↑
	Access Review conducted in the last year	58%	↑
	Documented Training Plan	97%	→
	Periodic Review of Roles and Responsibilities	97%	→
	Review of roles and responsibilities conducted in the last year	60%	↑
Internal Audit Tracking			
	Average Audit issues per audit project (Target value)	1.7 (1.9)	↑
	7 Days - Audit Responses	6,5	↓
	14 Days - Mitigating Controls Implemented	No Data	N/A
	30 Days - Detailed Action Plan for Sustainable Resolution	No Data	N/A
	90 Days - Action Plan Implemented	142	↓
Anti-Virus - Accountability			
	%Servers with Anti-Virus Installed	99.4% (3/521)	↓
	%Laptops & Workstations with Anti-Virus Installed	99.8% (40/17036	↑
	%servers with up to date definitions	98.5% (8/521)	↓
	%Laptops & Workstations with up to date definitions	95.7% (733/17036	↓
Security Patching - Accountablity			
	# of computers with out-of-date operating systems	57 (17557)	↑
	% up-to-date patches (>180 days)	99.2% (6261)	↑
	% up-to-date patches (<180 days)	98.0% (3911)	↓
Anti-Virus - Responsibility			
	%Servers with Anti-Virus Installed	100.0% (0/36)	→
	%Laptops & Workstations with Anti-Virus Installed	98.9% (8/716)	↑
	%servers with up to date definitions	97.2% (1/36)	↓
	%Laptops & Workstations with up to date definitions	95.5% (32/716)	↓
Security Patching - Responsibility			
	# of computers with out-of-date operating systems	9 (752)	↑
	% up-to-date patches (>180 days)	96.6% (977)	↑
	% up-to-date patches (<180 days)	94.9% (340)	↑

Tabla 3. Aspectos evaluados por las métricas

Cargill Beef Argentina	For More Antivirus/Security Detail -	Site Contact: Risk and Controls									
Business Unit Metrics	**June**	**July**	**August**	**September**	**October**	**November**	**December**	**January**	**February**	**March**
ARIS BIA Completion Average									**65%**	**65%**
ARIS - BIA Completed									100%	100%
ARIS - BIA Updated or Created in the Last Year									30%	30%
Archer BIA Completion Average									**0%**	**5%**
Archer - BIA Completed									0%	10%
Archer - BIA Updated or Created in the Last Year									0%	0%
Audit Follow-up										
Average Audit issues per audit project (Target value)	2,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0
7 Days - Audit Responses	8	8	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0
14 Days - Mitigating Controls Implemented	No Data	No Data	No Data	No Data	No Data	No Data	No Data	No Data	No Data	No Data
30 Days - Detailed Action Plan for Sustainable Resolution	No Data	No Data	No Data	No Data	No Data	No Data	No Data	No Data	No Data	No Data
90 Days - Action Plan Implemented	No Data	No Data	No Data	No Data	141,0	166,0	166,0	166,0	166,3	166,0
Anti-Virus - Risk Accountability										
%Servers with Anti-Virus Installed	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)
%Laptops & Workstations with Anti-Virus Installed	100.0% (0/272)	100.0% (0/270)	100.0% (0/290)	100.0% (0/263)	100.0% (0/265)	100.0% (0/274)	99.6% (1/261)	100.0% (0/266)	100.0% (0/271)	100.0% (0/269)
%servers with up to date definitions	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)
%Laptops & Workstations with up to date definitions	89.0% (30/272)	91.9% (22/270)	87.6% (36/290)	94.7% (14/263)	93.6% (17/265)	93.1% (19/274)	93.1% (18/261)	97.4% (7/266)	97.8% (6/271)	100.0% (0/269)
Security Patching - Accountability										
# of computers with out-of-date operating systems	0	0	3	0	0	0	0	0	0	0
% up-to-date patches (>180 days)	98,2%	97,8%	98.2% (87/4885)	98.6% (77/5612)	98.8% (68/5542)	98.9% (72/6799)	99.1% (67/7488)	98.3% (46/2710)	98.3% (45/2666)	98.2% (192/10905)
% up-to-date patches (<180 days)	**96,4%**	**96,9%**	98.1% (59/3059)	97.4% (56/2180)	97.4% (134/5235)	98.9% (64/5773)	99.0% (52/5031)	99.4% (61/10606)	99.4% (56/10157)	97.4% (76/2950)
Anti-Virus - Responsibility										
%Servers with Anti-Virus Installed	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)
%Laptops & Workstations with Anti-Virus Installed	100.0% (0/268)	100.0% (0/264)	100.0% (0/255)	100.0% (0/259)	100.0% (0/262)	100.0% (0/272)	99.6% (1/259)	100.0% (0/265)	100.0% (0/268)	100.0% (0/268)
%servers with up to date definitions	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)	100.0% (0/0)
%Laptops & Workstations with up to date definitions	89.2% (29/268)	92.0% (21/264)	87.8% (31/255)	94.6% (14/259)	93.5% (17/262)	93.0% (19/272)	93.1% (18/259)	97.4% (7/265)	97.8% (6/268)	100.0% (0/268)
Security Patching - Responsibility										
# of computers with out-of-date operating systems	0	0	3	0	0	0	0	0	0	0
% up-to-date patches (>180 days)	**98,2%**	**97,7%**	98.1% (82/4343)	98.6% (77/5498)	98.8% (68/5469)	99.0% (68/6716)	99.1% (63/7400)	98.3% (46/2689)	98.3% (45/2625)	98.8% (128/10740)
% up-to-date patches (<180 days)	**96,5%**	**96,9%**	98.5% (40/2690)	97.5% (53/2141)	97.5% (130/5171)	98.9% (64/5725)	99.0% (52/4989)	99.5% (57/10546)	99.6% (40/10014)	98.4% (46/2908)
Business Unit Supporting Documentation										

Risk Accountability - Machines owned by the BU regardless of who supports

Risk Responsibility - Machines owned by the BU, supported by the BU

Tabla 3. Reporte mensual de métricas.

Business Unit Metrics Report Period: March 2011		Cargill Beef	Cargill Beef Argentina
Business Impact Analysis			
	ARIS BIA Completion Average	**96%**	**65%**
	ARIS - BIA Completed	97%	100%
	ARIS - BIA Updated or Created in the Last Year	94%	30%
	Archer BIA Completion Average	**5%**	**5%**
	Archer - BIA Completed	10%	10%
	Archer - BIA Updated or Created in the Last Year	0%	0%
Audit Follow-up			
	Average Audit issues per audit project (Target value)	1,0	2,0
	7 Days - Audit Responses	7,0	8,0
	14 Days - Mitigating Controls Implemented	No Data	No Data
	30 Days - Detailed Action Plan for Sustainable Resolution	No Data	No Data
	90 Days - Action Plan Implemented	147,0	166,0
Anti-Virus - Accountability			
	%Servers with Anti-Virus Installed	97.0% (1/33)	100.0% (0/0)
	%Laptops & Workstations with Anti-Virus Installed	99.5% (13/2367)	100.0% (0/269)
	%servers with up to date definitions	97.0% (1/33)	100.0% (0/0)
	%Laptops & Workstations with up to date definitions	96.1% (93/2367)	100.0% (0/269)
Security Patching - Accountablity			
	# of computers with out-of-date operating systems	1	0
	% up-to-date patches (>180 days)	99.2% (827/104685)	98.2% (192/10905)
	% up-to-date patches (<180 days)	98.8% (324/26876)	97.4% (76/2950)
Anti-Virus - Responsibility			
	%Servers with Anti-Virus Installed	100.0% (0/0)	100.0% (0/0)
	%Laptops & Workstations with Anti-Virus Installed	76.2% (5/21)	100.0% (0/268)
	%servers with up to date definitions	100.0% (0/0)	100.0% (0/0)
	%Laptops & Workstations with up to date definitions	71.4% (6/21)	100.0% (0/268)
Security Patching - Responsibility			
	# of computers with out-of-date operating systems	1	0
	% up-to-date patches (>180 days)	30.7% (226/326)	98.8% (128/10740)
	% up-to-date patches (<180 days)	0.0% (63/63)	98.4% (46/2908)
Business Unit Supporting Documentation			

Tabla 4. Comparación de métricas entre diferentes BU.

Key:			
BIA	< 80%	80% - 90%	> 90%
Disaster Recovery	< 80%	80% - 90%	> 90%
Information Access Controls	< 70%	70% - 99%	> 99%
Internal Audit Tracking (Average Audit Issues per Audit Project)			
Internal Audit Tracking (7, 14, 30, and 90 day metrics)	Not meeting goals		Meeting goals
Anti-Virus Installed - %Servers & %Laptops & Workstations	< 95%	95% - 99%	>= 99%
Security Patching with patches greater than 180 days	x < 90%	90% - 99%	100%
Security Patching with patches less than 180 days	x < 90%	90% - 98%	>= 98 %

Tabla 5. Rango de calificaciones

Es importante mencionar, el Análisis de Impacto de Negocio se realizaba en otras plantas desde tiempo antes, en la BU se anexa a funciones y en un mes se logra estar no muy lejano a los trabajos que se realizaba en otras partes desde tiempo atrás. Se puede apreciar claramente el trabajo realizado comparado con Beef en el mundo, lo referente a la Unidad de Negocios Argentina es relativamente superior, mejora que continúa creciendo hasta transferir el Negocio.

3.6 Proceso de Comunicación de las Métricas en TGRC

Un metodología ineficiente o fallas en el proceso de comunicación también puede introducir nuevas amenazas al igual que la misma tecnología. De ello surge la necesidad del diseño de un plan de comunicación que acompañe eficientemente a las exigencias del agresivo proyecto **Tartan** y su componente **TGRC**. Se ha especificado que cambios en la composición de los equipos tecnológicos, en los procesos y las operaciones pueden producir cambios importantes que afecten a la organización. Fallas al comunicar los resultados, modificaciones o sus consecuencias contribuyen a incrementar el nivel de riesgo. Los métodos de comunicación, el conocimiento y el entendimiento o compresión por parte de los receptores, es fundamental si se pretende llevar adelante una exitosa gestión.

En el éxito de un proyecto de ingeniería, cuatro componentes esenciales se encuentran definidos en el proceso de comunicación:

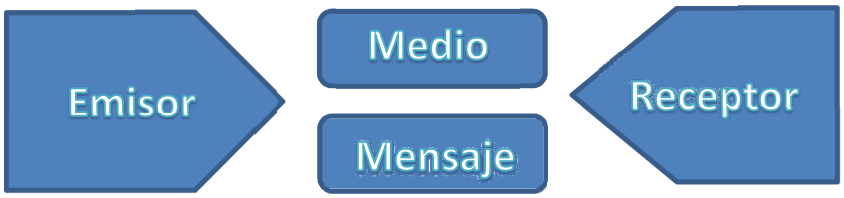


Figura 7. Componentes del proceso de comunicación.

En **TGRC**, el *emisor* estaba compuesto, para el caso del autor, directamente por el responsable global del equipo (Mr Bill Gabby) más todo su equipo de confianza y el autor era el *receptor* quien evaluaba los resultados junto al responsable y su equipo, estableciéndose los futuros pasos en el desarrollo del proyecto, esos pasos o acciones -en el marco de un plan global- muchas veces implicaban capacitación, orientación, elaboración de material guía y en ciertas ocasiones sanciones de carácter inflexibles. El *mensaje* tenía las características vistas en los reportes anteriores. Se desarrollará a continuación el *medio* como era distribuido mundialmente.

El *scorecard* o Tablero de Control es creado y comunicado mensualmente, poseyendo las siguientes características:

- Los datos usados para crear el *socercard* son recolectados de todas las PCs del mundo a medianoche (horario de Mineapolis) del día 15 de cada mes. Este proceso equivale a tomar una "fotografía", para ese punto, de todas las computadoras en el mundo. Si una laptop se encontraba apagada, el proceso se iniciará en el siguiente encendido. Esta "fotografía" la efectuaba el software ***Altiris***.
- Durante los pocos días siguientes, el scorecard es creado. El mismo es cargado en el sitio ***Punto de Servicios Compartidos*** de **TGRC**, pero aún no puede ser accedido por los analistas del mundo, pero sí por los integrantes del equipo central.
- Una reunión con Mr Chad Mead líder de Controladores de Plataforma, líderes de Plataforma, la oficina central de la organización del Plan **TGRC** y los TRCM (Technology Governance Risk Managers) de las Plataformas dispersas en el mundo es retenida o coordinada para el primer miércoles del mes (siguiente al punto de recolección de datos) para revisar y evaluar los indicadores para el mes observado, además de cualquier acción tomada u obstáculo de impacto surgido en el *scorecard*.
- Inmediatamente siguiente a la reunión con la Plataforma, el scorecard es compartido con los líderes senior de la empresa. Esto incluye al CEO, Mrs Rita Heise, y otros líderes de equipo en la empresa.

Aquí se puede incluir una importante información. Era falla importante tener una computadora de escritorio apagada por error o por evitar ser auditada. Mas aún, era falla considerada muy grave tener una computadora con el ***Altiris Agent*** detenido.

3.7 Roles y Responsabilidades

Como toda organización americana, el *scorecard* poseía roles bien definidos que no podían ser obviados o extralimitados.

En la siguiente tabla se listan los principales roles definidos para las cuatro áreas medidas dentro del reporte durante la recolección de datos, generación del reporte y su compartimiento con el resto de los equipos.

Actividad del *Scorecard*	BU/SSC IT Líder	Responsable App/IT	Líder BU	Controladores	TGRC
Recuperación Técnica/Recuperación de Desastres (DR)					
Completar/validar anualmente el Análisis de Impacto (BIA)	A	C	R	I, C	I, C
Completar el plan de Recuperación Técnica	A	R	C	I, C	I, C
Probar el plan de Recuperación de Desastre (DR)	A	R	C	I, C	I, C
Reportar acciones de prueba y resultados	A	R	C	I, C	R
Documentar brechas de riesgo observadas	A	R	I	I	I, C
Controles de Acceso a la Información					
Asegurar información TARTAN/ARIS(SW de inventario) actual	A	R	I	I, C	I, C
Completar el proceso de documentación y plantillas	A	R	I	I, C	I, C
Trabajar con la BU en los procesos estándar	A	R	I	I, C	I, C
Analizar la creación y el estado de acciones	A	R	I	I, C	R
Documentar brechas de riesgo observadas	A	R	I	I	I, C
Gestión de los Procesos de Auditoría					
7 días, Memo completado y publicado	I, C	R	I, C	I, C	A
14 días, Controles de Mitigación implementados/documentar	R	R	R	I, C	A
30 días, Plan de acción completado	A	R	I, C	I, C	I, C
90 días, Plan de remediación implementado	A	R	I, C	I, C	I, C
Actualizar IMC (Corpotate Audit Tracking)	I	I	A	R	I, C
Aplicar 'lecciones aprendidas'	A	R	I, C	I, C	R
Parches de Seguridad/Antivirus					
Instalar antivirus en los dispositivos de la empresa	A	R	I, C	I, C	I, C
Medir y analizar las tareas que necesitan ser completadas	A	R	I, C	I, C	R
Aplicar los parches de seguridad necesarios a los dispositivos	A	R	I, C	I, C	V
Gestionar, analizar y administrar las mediciones	A	R	I, C	I, C	R
Documentar brechas de riesgo observadas	A	R	I	I	I, C

A: Contable					
R: Responsable					
C: Consultor					
I: Informador					

Tabla 6. Definición de roles.

3.8 Software Encargado en de Recolectar Datos

Métrica	Sistema
Recuperación de Desastres (DR)	ARIS (Architecture of Integrated Information System)
Controles de Acceso a la Información	ARIS (Architecture of Integrated Information System)
Procedimientos de Auditoría	IMC (Corp. Audit Issue Management Center)
Seguimiento de Auditoría	IMC (Corp. Audit Issue Management Center)
Antivirus	ALTIRIS (Symantec)
Parches de Seguridad	ALTIRIS (Symantec)

Tabla 7. Software recolector de datos.

Archer Tool no se menciona aquí porque su utilización se relaciona al Resiliency Management (Gestión de Contingencias) y no con la recolección de datos, elaboración y divulgación de métricas.

RSA ARCHER®
CYBERSECURITY
FRAMEWORK
MANAGEMENT APP-PACK

4 ARCHER

4.1 Introducción al Software

En el presente trabajo se optó por realizar una descripción, entre todas las actividades y proyectos realizados, de lo que la empresa denominaba Resiliency Management Plan (Plan de Gestión de Contingencias). La herramienta de software más importante para promover la recolección de datos, elaboración del plan, prueba y documentación, estaba soportada por ***Archer Tool***.

Gobierno y Control de los Riesgos Tecnológicos (Technology Governance Risk & Control – **TGRC**) está implementando ***Archer***, una herramienta de software en la gestión de los riesgos, en la administración de los riesgos y en el seguimiento de la conformidad o cumplimiento de las metas definidas dentro de Cargill para el ambicioso proyecto, permitiendo contar con una tecnología simple en la plataforma gestión de riesgos que integre los datos desde múltiples herramientas.

La empresa poseía una firme convicción que podía administrar o direccionar mejor lo relacionado a los riesgos, asegurar una ayuda superior en el cumplimiento con las regulaciones y políticas globales, y evaluar mejor la posición de la empresa expuesta a los riesgos tecnológicos. Tanto los empleados como terceros contratados o clientes tenían acceso a la información almacenadas sobre las políticas de **TGRC**, obviamente los permisos de accesos a la información contenida eran cuidadosamente revisados

por, como el autor, cada uno de los analistas responsables de las Unidades de Negocios desplegadas en el mundo; también colaboraban en el trabajo mencionado los gerentes de Plataforma y Centro de Servicios Compartidos (SSC). Tarea que podía incluir adicionar un permiso de acceso a la información sensible, modificar o eliminar usuarios, pedir o solicitar accesos a otras soluciones o módulos en el software.

Archer, es desplegado en la empresa casi en coincidencia con la formación del equipo **TGRC**. Es actualmente el recurso donde van a parar todas las políticas sobre riesgo y control, mientras que el acceso a sus módulos está determinado por roles. Cada persona involucrada que tenía o podía llegar a tener acceso debería consultar a los analistas de riesgo y gerentes de control correspondientes, para determinar el rol que tienen o tendrán dentro de la herramienta, además de solicitar entrenamiento en el uso de la misma.

4.2 Aproximación de Archer a TGRC

Con la atención reciente de los medios y la conciencia de los consumidores sobre fallas corporativas tales como violaciones de datos, violaciones de cumplimiento e interrupciones comerciales, los ejecutivos y miembros del CEO han aumentado su escrutinio y se han involucrado más en iniciativas de gobernabilidad, riesgo y cumplimiento. Después de todo, si un riesgo operacional, incumplimiento importante o problema de conformidad afecta a su empresa, será su reputación, e incluso sus trabajos en la línea quienes se vean seriamente dañados.

La gestión de un cambio cultural desde el control reactivo de los sectores involucrados para el cumplimiento hasta un modelo de gestión de riesgos más proactivo requiere cambios y participación en toda la organización. Si se intenta abordar todo a la vez, puede tocar un gran porcentaje del negocio, pero no tener la profundidad para desarrollar procesos efectivos. Incursionar en un área extensas podrían dejar a otras partes de la organización expuestas.

El riesgo está cambiando tan dramáticamente que ya no se puede mirar hacia el pasado para determinar los próximos pasos. Desde el ciber-riesgo hasta las regulaciones, la velocidad creciente y la naturaleza más amplia de los riesgos de la globalización y la competencia en el mercado se vuelven aún más complejos por los intentos de piratería más ingeniosos y la intervención agresiva del gobierno. Los procesos manuales dificultan la obtención rápida de información a los interesados. Desde problemas de control de versiones hasta métodos inconsistentes de medición, esta información dispersa se convierte en un obstáculo para remediar el riesgo. Incluso

las soluciones puntuales más exitosas solo exacerbarán este desafío, ya que la información se almacena en diferentes lugares y se usa de diferentes maneras en cada departamento.

Si no se puede reducir los incidentes de riesgo y cumplimiento en cada unidad de negocios, seguramente nos enfrentaremos a preguntas difíciles sobre la relevancia del programa de **TGRC**. Peor aún, un evento de riesgo importante podría poner en peligro la reputación de la marca y la confianza del consumidor, permitiendo que los competidores salgan adelante.

RSA Archer® Análisis de Impacto de Negocio, está diseñado para ayudar a determinar la criticidad de los procesos comerciales. Se puede compartir información con equipos interdependientes en toda la organización y permitir que los líderes empresariales prioricen estrategias de recuperación, tareas de recuperación, evaluaciones de riesgos y otras actividades cruciales para las operaciones de toda la empresa y los sistemas de IT.

El Ecosistema ARCHER

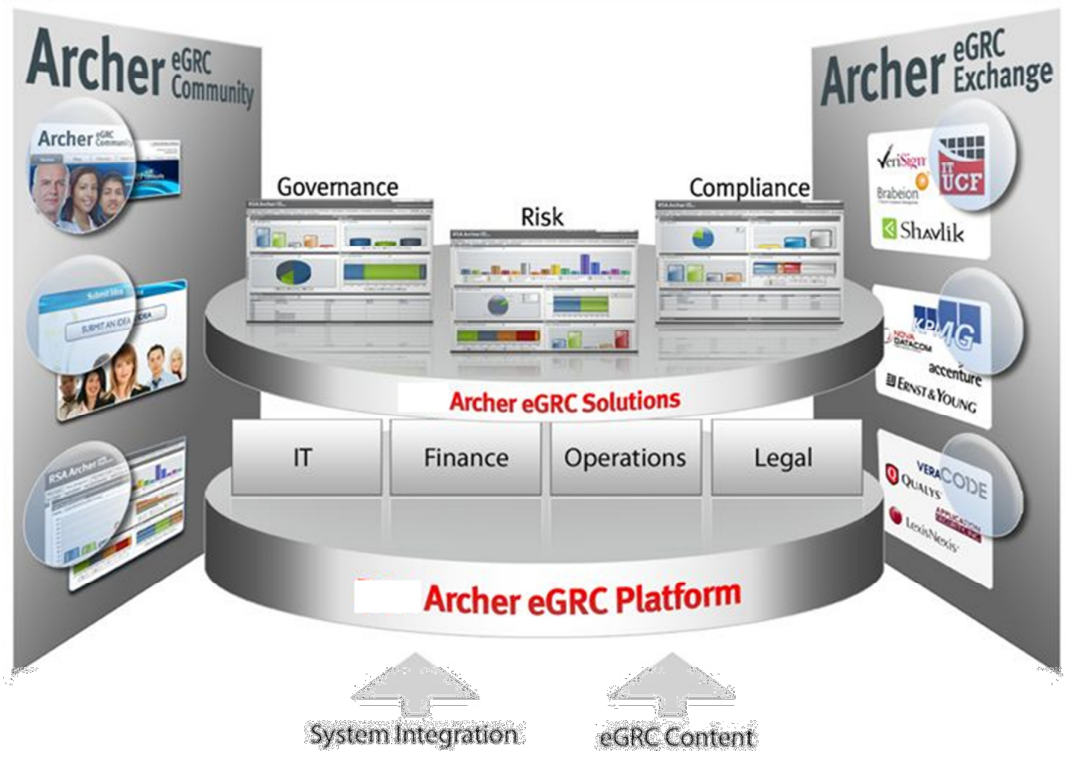


Figura 8. Ecosistema Archer.

El éxito de la plataforma ***Archer*** en **TGRC** comienza con una base tecnológica común para su programa de riesgo y cumplimiento. La plataforma ***Archer*** crea un conjunto común de capacidades, metodologías y taxonomía para su programa de riesgo y cumplimiento. Esto permite una mayor integración de sus datos en su programa, mientras crea un lenguaje común y una estructura de informes para compartir resultados.

Dentro del contexto empresarial, la organización debe saber qué activos afectan su negocio, cómo están relacionados, quién es responsable del activo y cuál puede ser la prioridad del negocio. Con ***Archer***, la organización puede catalogar su estructura organizacional e infraestructura operativa. Esto le permite formar una vista global del negocio, determinar el valor de la infraestructura de soporte y usar esa información para priorizar los riesgos o controles que requieren atención inmediata.

4.3 Principales Características

- Incluye un catálogo de definición de procesos en la empresa y un análisis de impacto en la organización construido con flujo de trabajo, notificaciones y datos de referencia para determinar la criticidad de todos los procesos comerciales.
- Los propietarios de los procesos de negocios o los equipos de gerentes de control de negocios (BCM) pueden iniciar una actualización del BIA dependiendo de la clasificación de criticidad del proceso, la fecha de la última modificación del BIA u otros factores.
- El equipo BCM puede comenzar una campaña para iniciar BIA para múltiples procesos de negocios en la Unidad de Negocio (BU), o aquellos que respalden el lanzamiento de un nuevo producto o servicio.
- Lo roles de acceso son provistos por los propietarios responsables de la administración BIA para la BU correspondiente, equipos de BCM y ejecutivos que conducen fácilmente su flujo de trabajo de finalización, revisión y aprobación del flujo de trabajo BIA para cada uno.
- Todos los BIA cargados deben ser aprobados por el equipo central de **TGRC** en Mineapolis. Si alguno estuviese incorrecto o incompleto, se genera un reporte desde el CEO y se promueve e induce su modificación para alinearse a las metas u objetivos globales de la organización.

4.4 Principales Beneficios

Con **Archer** Analisis de Impacto de Negocio, podemos dentro de la empresa:

- Implementar un sistema consolidado de registro para todas las BIA.
- Utilizar un enfoque único para completar BIA con flujo de trabajo, notificaciones, procesos de revisión y aprobación.
- Proporcionar informes que muestren las métricas clave e informes para permitir que los equipos de BCM, los gerentes de las unidades de negocio y los gerentes de procesos comerciales administren sus BIA. Aunque en el caso de Beef Argentina, la responsabilidad recaía solamente sobre el Analista responsable y el equipo central de **TGRC**.

4.5 Principales Funcionalidades

Se listarán a continuación algunas funcionalidades del software:

- ***Gestión de riesgos de IT y seguridad.*** Las nuevas y emergentes amenazas de IT y de seguridad son omnipresentes en los negocios complejos de hoy en día. Con ***Archer***, se puede determinar qué activos son críticos para el negocio, establecer y comunicar políticas y estándares de seguridad, detectar y responder a ataques e identificar y remediar deficiencias de seguridad. Esto permite reducir el riesgo de amenazas de seguridad, prácticas deficientes o desalineadas y fallas en el cumplimiento de la seguridad operacional.
- ***Gestión regulatoria y de cumplimiento corporativo.*** Con la constante afluencia de nuevas y cambiantes regulaciones, la empresa necesita comprender qué regulaciones son relevantes. Ahora la organización puede establecer el contexto comercial para el cumplimiento, identificar y cumplir con las obligaciones regulatorias, establecer e implementar políticas y estándares de conformidad, o bien crear y administrar un marco de control integrado. Esto no solo reduce el riesgo de malas prácticas de IT o procesos comerciales mal alineados, sino también la exposición a infracciones normativas y su funcionamiento.
- ***Gestión de riesgos empresariales y operacionales***. Los existentes enfoques de gestión de riesgos ad hoc a menudo abruman a los equipos de gestión de riesgos y no proporcionan una imagen de riesgos constante y en tiempo real para el equipo ejecutivo y consejo. Al implementar la herramienta en toda la organización, se puede comprender el contexto comercial para el riesgo operativo, identificar, evaluar y rastrear riesgos emergentes y operacionales, establecer políticas y estándares e implementar y monitorear los controles operativos. Además, proporciona la base para extender los procesos de

administración de riesgos operativos a seguridad, flexibilidad, cumplimiento normativo, auditoría y políticas de terceros.

- ***Contingencias en la Unidad de Negocio (BU)***. Desafortunadamente, pueden ocurrir eventos imprevistos y la organización deben estar preparada. Comprender qué activos son críticos para la restauración durante una crisis es imperativo para la supervivencia del negocio. La herramienta permite a la organización prepararse para las interrupciones de IT y comerciales, catalogar y resolver incidentes operacionales, y administrar eventos de crisis y comunicaciones. Esto reduce el riesgo en aquellas interrupciones de IT y comerciales, eventos operacionales nocivos y crisis comerciales importantes.
- ***Gestión de Auditorías***. Las auditorías desempeñan un papel fundamental como tercera línea de defensa al proporcionar seguridad independiente de los objetivos de riesgo y cumplimiento. La herramienta permite controlar el ciclo de vida completo de la auditoría, lo que permite una mejor gobernanza de las actividades relacionadas con la auditoría, a la vez que proporciona integración con sus funciones de control y riesgo. Se puede transformar la eficiencia del departamento de auditoría, completar auditorías de mayor alcance más rápidamente y disminuir los honorarios de auditoría externa.
- ***Gobernabilidad de terceros.*** El riesgo de terceros se presenta de muchas formas, incluida la seguridad de la información, la continuidad o simplemente perdida de productos o servicios de los que depende la empresa. Con la herramienta, la organización puede administrar todo el ciclo de vida de terceros en interacción con la propia empresa. Esto incluye reducir los riesgos heredados de terceros en la empresa extendida y la cadena de suministro, así como monitorear el desempeño de vendedores y proveedores clave.

4.6 Modo de Utilización

El modo de utilización, una vez definidos los procesos y subprocesos, áreas, principales actividades y responsables entre otras características, se ingresa iniciando sesión:

Figura 9. Logueo en Archer.

- *Iniciar sesión* indicando usuario, empresa y contraseña.
- *Completar* los procesos y subprocesos indicados, sus áreas de aplicación, valuación monetaria, y muchos otros datos más.
- *Guardar* las cargas o modificaciones a procesos existentes.
- *Cargar* si no se necesita generar ningún otro dato más. La carga implicaba que se encuentre disponible para ser revisado y evaluado, lo que aconsejaba un minucioso chequeo antes de proceder a este paso para evitar no solo trabajo al equipo principal, sino también evitar reiteradas observaciones que generarían sanciones.
- *Cerrar la sesión* iniciada.

4.7 Formato Gráfico

La herramienta posee un formato muy gráfico, amigable e intuitivo de trabajo. A continuación, se puede apreciar las principales funcionalidades.

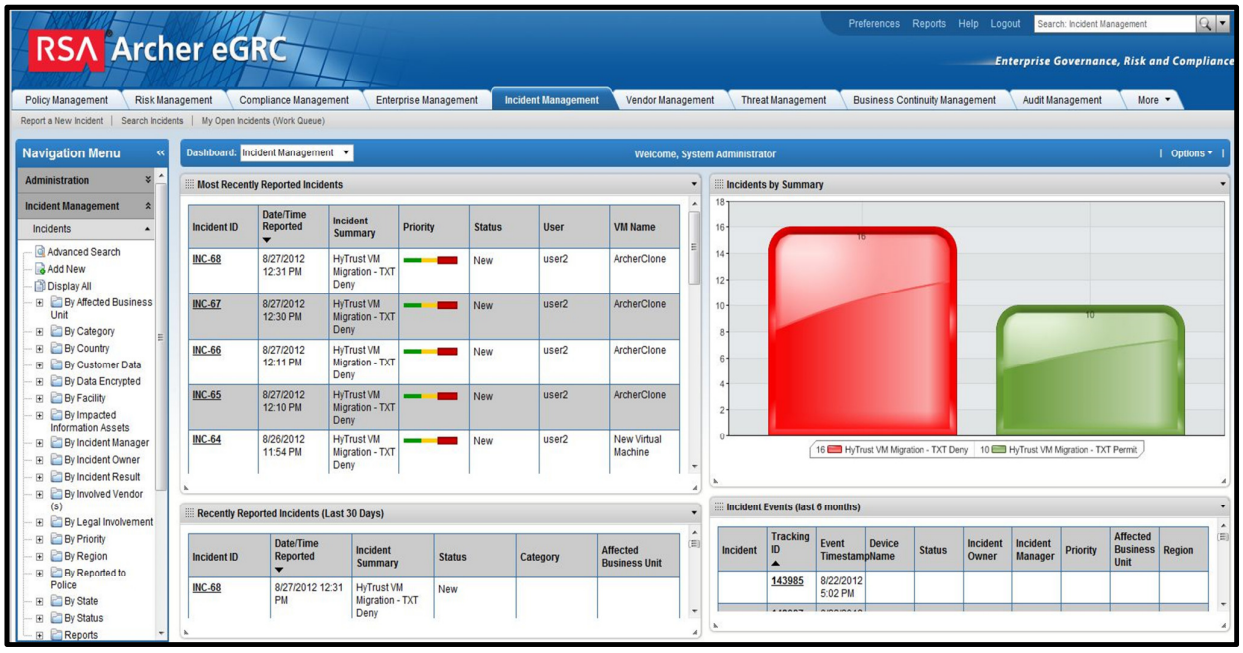


Figura 9. Ejemplo: Módulo Gestión de Incidentes.

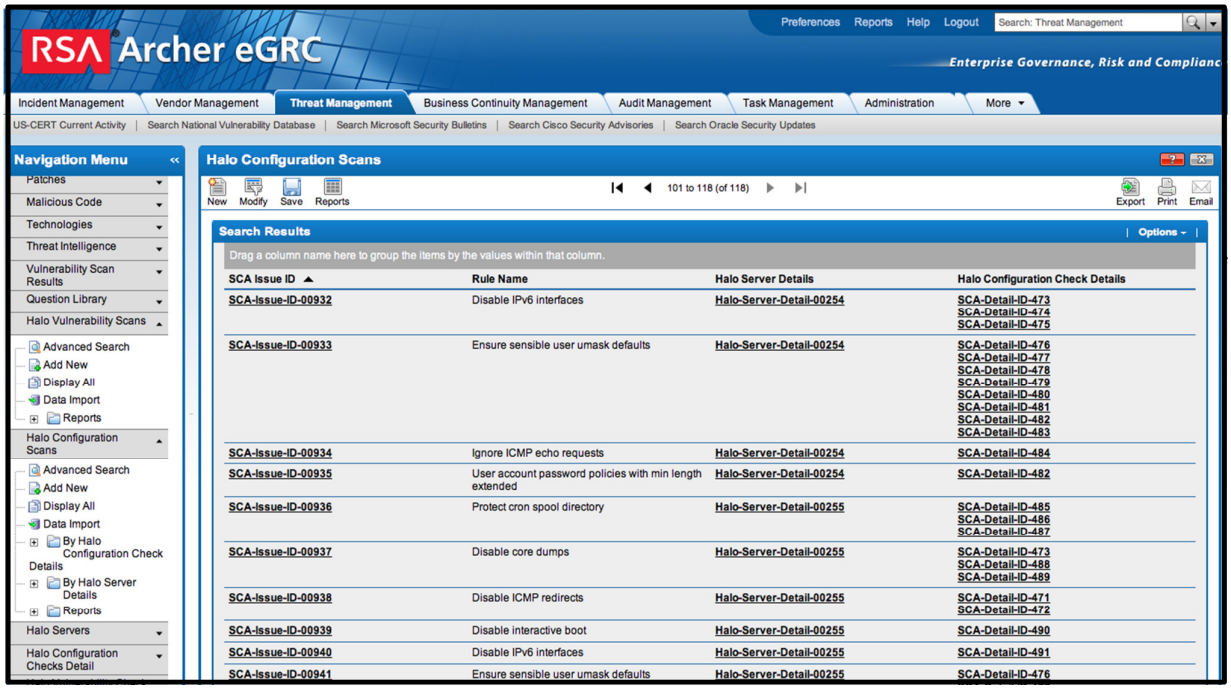


Figura 10. Ejemplo: Módulo Gestión de Amenazas Detectadas.

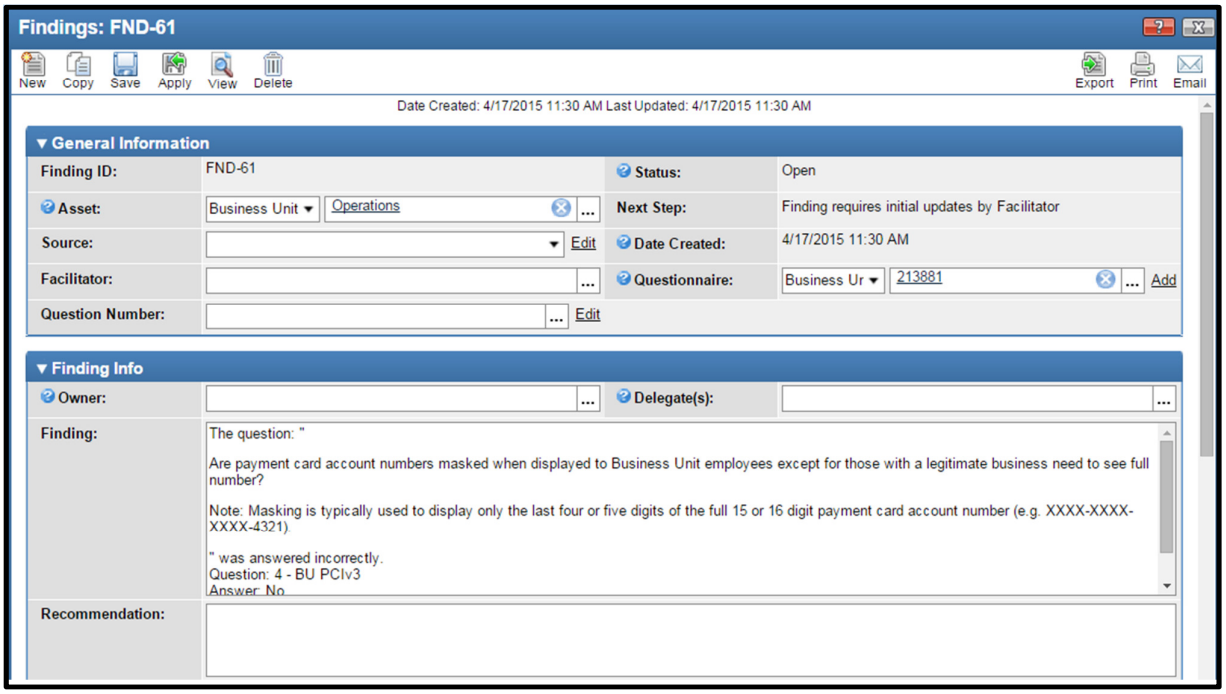


Figura 11. Ejemplo: Módulo Carga de Proceso.

Se puede observar que navegar dentro de la herramienta es muy fácil, el recaudo se debe tener en la carga de los datos al momento de completar el registro.

4.8 Ruta de Acceso al Proceso de la Organización

Se describirá la forma en que la herramienta maneja los registros y el árbol de jerarquías de módulos.

Si selecciona un Proceso Comercial en la organización de referencia, ***Archer*** rastrea la ruta de regreso al registro de la Unidad de Negocio (tanto directa como indirectamente) para determinar cuántos registros de evaluación crear por despliegue. Una vez que se crean los registros de evaluación, ***Archer*** luego determina todos los Riesgos y Controles vinculados directa o indirectamente a esos registros del Proceso Comercial.

Nota: solo la aplicación de Registro de Riesgos es incluida como parte del esfuerzo de definición del alcance. Gestión de la Continuidad de Negocio (BCM) tiene su propia aplicación de registro de riesgos, que no es inclusiva. Los riesgos vinculados a la Unidad de negocios a través de un compromiso de auditoría o incidente, no están incluidos en la ruta del alcance. Es decir, esos datos los extrae de otro enlace más complejo que no será incluido en el presente trabajo.

La jerarquía modular de los procesos de negocio en la aplicación se aprecia en el siguiente gráfico:

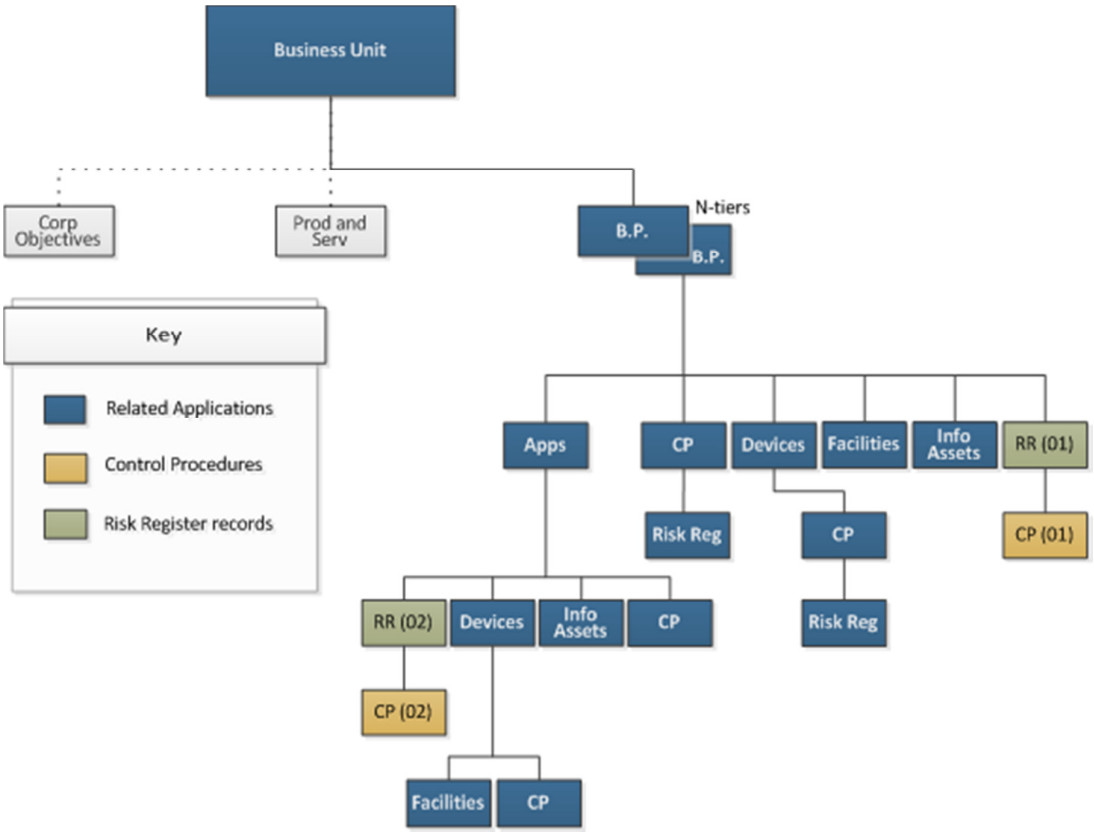


Figura 12. Árbol de registros dentro de Archer.

5 IDENTIFICACIÓN DE PROCESOS Y SUBPROCESOS

5.1 La razón por la que definimos Procesos y Subprocesos

En el entorno industrial y comercial de hoy, todas las empresas deben operar en una economía global en la que la competencia se hace cada vez más difícil y las expectativas de los clientes aumentan continuamente. Como resultado, las empresas deben exprimir sus negocios para obtener eficacia y eficiencia ofreciendo los resultados comerciales esperados, al tiempo que aumentan la calidad y la flexibilidad para satisfacer las expectativas de sus clientes.

La empresa de referencia no estaba ajena a estas circunstancias. Estas presiones junto con una recesión global en los años 80 y principios de los 90 llevaron a la creciente popularidad en Estados Unidos (US) sobre la definición de Procesos, suplantando la orientación a las aplicaciones como hasta ese entonces. Los conceptos y principios detrás de Gestión Total de Calidad motivaron a las empresas a enfocarse y examinar críticamente sus procesos comerciales con el objetivo de lograr pequeñas mejoras paso a paso, orgánicamente, a través de la aplicación de herramientas y técnicas rigurosas.

Aunque la Gestión Total de Calidad creó cierta cantidad de enfoque en los procesos comerciales, la importancia y el valor de la orientación de los procesos comerciales no se apreció hasta la publicación de lo que ahora se consideran los documentos fundamentales sobre el tema de la Reingeniería de Procesos Empresariales (BPR[23]) de Michael Hammer en 1990 (Hammer, 1990). El enfoque de Hammers hacia BPR, al

[23] Business Process Reengineering

contrario del enfoque orgánico de Gestión Total de Calidad, sugiere un mirada mucho más radical y descendente para la reingeniería de los procesos de negocio.

Desde su inicio, BPR ha ido creciendo en popularidad. Particularmente el enfoque descendente ha sido usado por la empresa de referencia en lo que es la identificación de Procesos y Subprocesos

5.2 Diseño Descendente Orientado a Procesos

Un enfoque orientado al proceso para la transformación a través de la adopción de tecnología es la clave en situaciones dinámicas tales, enmarcando en el tema a la compañía. Lo referenciaremos como el enfoque de "arriba hacia abajo", recomendado a las organizaciones que se embarcan en un viaje de transformación en varios niveles de madurez. Además, este enfoque ayuda a las organizaciones a evaluar su estado actual, establecer metas de transformación y trazar un plan realista y sostenible para llevar a cabo la gestión del proceso de extremo a extremo, *de una idea a la realidad*.

La transformación orientada a procesos requiere una visualización nítida del entorno de IT organizacional como una colección de procesos de negocios, en lugar de una colección de sistemas y funciones. La vista sistémica de una organización a menudo da como resultado decisiones de IT inapropiadas. Pero los enfoques orientados al proceso se centran en el desarrollo y la gestión integral de la arquitectura de procesos de la organización (una jerarquía de procesos de extremo a extremo diseñada para crear valor por y para el cliente) en lugar de una mejora fragmentaria de una función o sistema específico.

Falta de propietarios de los procesos
Falta de coordinación Negocios/IT
Falta de habilitación BPM[24] de los principales usuario de Negocios y IT

Falta de casos de negocios alineados
Inapropiada priorización de los procesos para la implementación
Ausencia de mapa BPM

BPM pareciera un proyecto de un tiempo y no como de continua mejora
Inapropiada selección de tiempo para los procesos de producción en serie

Figura 13. Principales desafíos en la empresa

[24] Business Process Management

Estudios anteriores en la empresa determinaron que un alto porcentaje de las organizaciones para ese momento, y muchas aún hoy, adolecen de las falencias enunciadas en el cuadro anterior solo por nombrar algunas.

Por lo tanto, utilizar un enfoque de arriba hacia abajo en el negocio describe un estilo de organización tradicional que enfatiza los imperativos y la visión de la alta gerencia. Las directivas y los objetivos de la organización descienden desde la parte superior hacia abajo.

5.3 Reingeniería de Procesos, la Apuesta de la Empresa

La reingeniería de procesos de negocios implica el rediseño radical de los procesos centrales del negocio para lograr mejoras drásticas en productividad, tiempos de ciclo y calidad. Aquí, la empresa comienza con una hoja en blanco y replantea los procesos existentes para ofrecer más valor al cliente. Por lo general, adoptábamos un nuevo sistema de valores que pondría mayor énfasis en las necesidades del cliente. La empresa reduciría las capas organizativas y eliminaría las actividades improductivas en dos áreas clave. Primero, rediseñaríamos la organización funcional en equipos interfuncionales. Segundo, usaríamos la tecnología para mejorar la diseminación de datos y la toma de decisiones.

Cómo funciona, en la organización, la reingeniería de procesos empresariales:

La reingeniería de procesos de negocios es una iniciativa de cambio dramático que contiene cinco pasos principales que los gerentes y responsables deben llevar a cabo:

- Reenfoque los valores de la compañía en las necesidades del cliente.
- Rediseñar procesos centrales, a menudo utilizando tecnología de la información para permitir mejoras.
- Reorganizar un negocio en equipos interfuncionales con la responsabilidad de principio a fin para un proceso.
- Repensar cuestiones básicas de la organización y las personas.
- Mejorar los procesos de negocios en toda la organización.

Durante los años posteriores a 2007 era común recibir correo electrónico dirigido a ciertos empleados con preguntas tales como:

- Cómo considera usted que podemos mejorar determinado proceso.
- Cómo considera usted que podemos agregar valor a determinado producto.

- Cómo estima podríamos llegar a darle un valor a nuestros productos que los hagan elegidos, por clientes, dentro de las opciones similares en mercado.
- Proponga ideas innovadoras que sean aplicables en la compañía y no se contradigan ni con la misión de la empresa ni con los principios guía.

Al integrar el equipo **TGRC**, el autor toma dimensión de los agresivos y ambiciosos cambios planteados para los años posteriores dentro de la organización en toda su estructura.

5.4 La Apuesta de TGRC al Usar la Metodología

El enfoque descendente se basa en las construcciones antes mencionadas, implementando la metodología, la empresa intentará sacar provecho de los siguientes principios claves:

• Articulación clara de objetivos y metas de negocios inteligentes, impulsados por los resultados deseados centrados en el cliente entregando el valor requerido por los mismos.

• Evaluación correcta del panorama actual para comprender la madurez y la capacidad de la organización para entregar programas de transformación digital habilitados con BPM.

• Identificación de las iniciativas correctas necesarias para alcanzar el nivel deseado de madurez y capacidad.

• Identificación y priorización de los procesos y la tecnología correctos para obtener el resultado comercial deseado.

• Creación de una hoja de ruta alcanzable y de varios períodos, con objetivos claros que abarcan:

- Iniciativas necesarias para aumentar la madurez y la capacidad de ejecución.

- Programas BPM para implementar los cambios deseados para procesos seleccionados.

Se iniciaba el proceso tomando como base “una hoja en blanco”. Analogía usada para indicar partir de cero, de la nada misma, de una compresión del negocio que permita determinar:

- Que hacemos?
- Como lo hacemos?

Sin caer en el error de preguntar: por qué lo hacemos así?. En una empresa global, de las dimensiones de la compañía en estudio, más aún con la cantidad de Unidades de Negocios que se incorporan, la Reingeniería de Procesos de Negocio es una herramienta valiosísima que permite conocer e incursionar en procesos de negocios desconocidos para la organización central, modelarlos y optimizarlos, alineándolos a las nuevas exigencias de eficiencia de mercado. Anteriormente un producto puesto en determinado sector debía estar dentro de los parámetros de calidad, hoy no basta este concepto, hoy debe tener un valor agregado que nos haga -como empresa- la mejor elección que tiene el cliente dentro del rubro en que competimos.

Esta tarea nos involucraba a todos los empleados que conformábamos la organización.

Una definición correcta de los procesos de negocio, puntapié inicial para posteriores cambios, permitirá dentro de la empresa proveer a las actividades de una mayor eficiencia a través de la reingeniería de procesos.

5.5 TGRC y los Pasos en la Identificación

El componente principal del Plan de Gestión de Contingencia (Resiliency Management) era la identificación de los Procesos de Negocio, los Subprocesos que lo componen y dentro de ellos se encontraban definidas un número finito de actividades, así como las áreas que afectaba el proceso y herramientas de software utilizadas.

Una correcta definición continuaba con una valoración monetaria del proceso-subproceso, un tiempo máximo de tolerancia que significaba tenerlo inoperante, un punto deseable de restauración, un punto óptimo de recuperación, etcétera.

La definición de un proceso se iniciaba con una reunión con el responsable del sector (contaduría, logística, producción y laboratorio, solo por nombrar algunos). Las reuniones tenían previsto un mínimo de 30 minutos y un máximo de 1 hora. En ella, siguiendo un patrón de preguntas preestablecidas se delineaba el conjunto de *Major Precesses* (Procesos Principales). Una vez definidos los mismos, se ingresaba en la

identificación de todos los *Subprocesses* (Subprocesos) que formaban parte del proceso principal.

Cargill contaba con una definición de *13 Major Processes* y *más de 100 Sub-Processes* dentro de los cuales se podían definir todos los procesos existentes en todas las unidades del mundo. En tanto para las actividades que incluía, se tenía una guía de como expresarlas en inglés de un modo fácilmente interpretado por la gerencia en Mineapolis.

5.6 TGRC y los Procesos Preestablecidos

La empresa tenía definido 13 procesos principales (*Major Processes*) a los cuales los encargados de las Unidades de Negocio, para el Proyecto **Tartan**, se debían alinear.

A continuación, se detallan los mismos con su número de identificación y su descripción:

ID #	Nombre Proceso Principal	Descripción
1	Registrar para Reportar	Uno de los once principales procesos que cubren la estrategia de informes, la contabilidad financiera y de gestión, y los impuestos / aduanas y otros informes gubernamentales.
2	Alinear a la Empresa	Uno de los principales procesos que establece las bases para que las unidades de negocio, funciones, plataformas y procesos de negocios se alineen.
3	Planeamiento y Gestión de los Servicios en la Empresa	El proceso principal que incluye procesos que son procesos estándar en toda la empresa, así como los procesos de infraestructura que respaldan y permiten las diversas estrategias en todos los negocios de la empresa a lo largo del mundo.
4	Orden de Cobro	Orden de Cobro es el proceso de capturar pedidos de clientes, comparar parámetros de pedidos con los parámetros contractuales del cliente, validar los requisitos de crédito del cliente, coordinar el procesamiento y entrega del pedido según los requisitos del cliente, facturar al cliente y cobrar el importe facturado. Este proceso también incluye proporcionar soporte y servicio para consultas de clientes relacionadas con el seguimiento de pedidos, quejas, resolución de disputas, preguntas relacionadas con productos, facturación y respaldo crediticio. El cumplimiento del pedido generalmente es respaldado por otras funciones como operaciones, logística y almacenamiento.

5 y 6	Comercio a Ejecutar (usado para ambos casos)	Uno de los doce principales procesos que representan el inicio del ciclo de vida de un contrato comercial u operación de futuros / opciones. Comercio a Ejecutar, cubrirá las actividades de compra y venta comercial que tienen un riesgo de mercado y requieren un proceso de contratación. El proceso principal de Comercio para ejecutar comienza con el desarrollo de un sesgo comercial basado en el análisis de una serie de información de propiedad y externa. Se aplica a la primera compra / manejo de varios insumos (generalmente productos básicos) que se venderán o procesarán y se extenderá a cuando la empresa venda a un tercero o una instalación de la propia empresa procese estos insumos en productos de mayor valor. En casos seleccionados, también se extenderá a los productos de las instalaciones de procesamiento que tienen diversos riesgos de mercado y un sistema de contratación. El proceso de transacción para ejecutar los contratos de compra y venta comercial cubre la grabación, modificación, fijación de precios, rotación de fechas de entrega y cancelaciones. También incluye la confirmación de los términos y condiciones del contrato con la contraparte para verificar / validar el contrato.
		Los contratos comerciales de compra y venta incluyen una serie de productos que se venderán o procesarán, incluidos (entre otros): trigo, cebada, malta, avena, maíz, sorgo, soja, harina de soja, aceite de soja / aceite de semilla suave (grado de refinación por definir), softseeds, NGFI, fletes marítimos de carga / tiempo fletes, carga de barcazas, azúcar, algodón, productos ferrosos comercializados, granos de cacao / mantequilla / polvo, harina, subproductos de empresas de procesamiento con riesgo de mercado, jugo , aceite de palma (grado de procesamiento por definir), ganado, cerdos, productos de cvam, carbón, biocombustibles, petróleo (crudo y productos), electricidad, gas natural, otros intercambios de efectivo de energía, intercambios de TSF y CRM, insumos de fertilizantes - NPK. Esto incluye desarrollar, optimizar y ejecutar un plan para la adquisición, comercialización, venta e intercambio de estos materiales, así como también la gestión de riesgos asociada con estas transacciones.
7	Desarrollar productos, servicios, soluciones	El proceso de desarrollo de Productos / Servicios / Soluciones produce diseños de productos comercializables y servicios que satisfacen las necesidades y deseos de los consumidores y clientes. Estos productos y servicios surgen de un conocimiento profundo de las necesidades del cliente y del entorno comercial. El proceso está impulsado por estrategias coordinadas de marca / categoría y segmento. Está respaldado por: - investigación (consumidor, cliente y competidor) - Inteligencia de marketing (el producto debe ser el correcto para el mercado e introducido en el momento adecuado) - enfoque estructurado (respaldado por el costeo objetivo y la expectativa de rendimiento frente a las necesidades del mercado).

8	Comercio y Mercado	Los productos y servicios de" marketing" implican el análisis del mercado y el desarrollo de estrategias. Estos incluyen análisis de la competencia, identificación de clientes, identificación de oportunidades de comercialización y desarrollo de las siguientes estrategias: fijación de precios, acceso al mercado, publicidad, relaciones públicas, canal de distribución física, fuerza de ventas y estrategia de servicio al cliente. Los procesos de ventas incluyen todas las actividades de planificación de ventas, ventas directas, gestión de intermediarios, evaluación de la fuerza de ventas y actividades de soporte de ventas. También se incluyen el diseño e implementación de Internet y del centro de llamadas.
9	Plan a Producir	Uno de los once principales procesos que representan la definición de la estrategia de fabricación para la disposición del producto y el seguimiento del rendimiento de fabricación. Además, también se incluyen las jerarquías de planificación de definición y ejecución, el procesamiento de las actividades / datos de fabricación en los sistemas de información y la inspección del producto.
10	Procurar el Pago (Cobrar)	Toda tarea o proceso neta y exclusivamente destinada al cobro.
11	Contratar el Retiro	Todos los procesos asociados con la gestión de un ciclo de empleado se contratan en la organización, la progresión de la carrera, a través de la jubilación o la salida.
12	Gestión del Movimiento y Almacenamiento de Mercancías	Incluye todas las actividades comerciales necesarias para planificar, mover y gestionar el flujo de mercancías entre el origen y el destino, incluidos los productos básicos, las materias primas y los productos terminados. Debido al alto volumen de transacciones físicas, este es un proceso clave en Cargill. Cubrirá todos los modos de transporte, incluida la carga de camiones terrestres, menos de camiones, ferrocarriles, buques oceánicos, contenedores, barcazas y aire. Incluye la coordinación del envío, entrega y recepción de productos de proveedores y / o clientes, almacenamiento, recolección, embalaje, etiquetado y carga, así como la administración y el seguimiento de los niveles de inventario físico en varias ubicaciones y los pagos y auditorías asociados al servicio proveedores. El proceso incluirá la administración y el mantenimiento de los activos físicos propios y arrendados y el equipo utilizado para el almacenamiento y / o movimiento. El proceso también incluirá el desarrollo de políticas para lidiar con servicios de terceros como corretaje, fumigación, limpieza y mantenimiento de autos, bultos, etc. Esta estrategia se basa en la recopilación, diseminación y análisis de los datos creados a partir del proceso. incluyendo hacer recomendaciones para mejoras.

13	Gestión de las Relaciones Comerciales (Ventas)	Este proceso incluye todas las actividades de planificación de ventas, ventas directas, gestión de intermediarios, evaluación de la fuerza de ventas y actividades de soporte de ventas.

Tabla 8. Procesos Preestablecidos por Tartan.

5.7 Tecnología Usada por Proceso

Una vez que identificábamos los procesos, el paso siguiente era muy simple. Solamente debía establecer la tecnología/las tecnologías que eran utilizada/s para desplegar el proceso dentro de la organización. En la siguiente tabla se muestra una identificación real realizada en el marco de **Tartan** para un proceso determinado.

			Technology Used									
Major Process	Proces No.	Process Name	Technology 1	Technology 2	Technology 3	Technology 4	Technology 5	Technology 6	Technology 7	Technology 8	Technology 9	Technology 10
RTR	1,22	Manage Corporate Budgeting/Forecasting	JDE World	Regional Finance Excel Models	PowerPoint	Excel	Enterprise Asset Management Tool Suite					
ATE	2,06	Manage and Improve Enterprise Performance	Microsoft SharePoint	Intranet	Audio/Web Conferencing		Excel	Word	PowerPoint	Email	ITSM	Altiris
PMES	3,01	Define Business Strategy	Excel	PowerPoint	Outlook	Sharepoint						
PMES	3,02	Define Business Plan	Excel	Powerpoint	Outlook	Sharepoint						
PMES	3,06	Manage IT Services	altiris	Insight License Advisor Tool	Cargill's IT Framework Website	Audio/Web Conferencing	Service Management Process Tools	Dell Portal	A&D Lab	ITO Paging	Email	Instant Messaging

Tabla 9. Tecnologías usadas por el Proceso.

5.8 TGRC y la Simplificación de Procesos

El análisis de valor de proceso implica una revisión de cada paso de un proceso para ver si la actividad proporciona valor al cliente. Si la actividad no proporciona valor, el equipo de análisis, el cual integró el autor, busca formas de eliminarlo del proceso. Al realizar un análisis exhaustivo del valor del proceso, una empresa puede eliminar costos de la organización y acortar la duración del proceso. Cuando se reduce la duración de un proceso, los clientes experimentan un menor tiempo de respuesta para sus pedidos, lo que aumenta los niveles de satisfacción del cliente.

Los procesos pueden someterse a análisis repetidos de este tipo, donde las últimas tecnologías y equipos se pueden aplicar a la última iteración de un proceso. El concepto también es aplicable a negocios adquiridos, donde la empresa puede presupuestar reducciones de costos probables en la nueva Unidad de Negocios a partir de un conjunto amplio de análisis de valor de proceso. En su momento la empresa de

referencia realizó el *due diligence* (del que participó el autor) para determinar si era "negocio" adquirir otra compañía, el resultado fue que para estandarizar los procesos a las exigencias de la empresa era más el desembolso que la ganancia a corto plazo.

En principio, este análisis puede parecer una excelente manera de mejorar varios aspectos de una organización, pero existe el riesgo de que se eliminen los puntos clave de control de un proceso en la búsqueda de reducciones de costos. En consecuencia, el personal de contabilidad o un analista de controles se incluían en el análisis para asesorar sobre cómo retener controles sólidos.

5.9 TGRC y la Valoración de los Procesos

Una vez que se identificaban los procesos y subprocesos que constituían o integraban la empresa, como también efectuado las simplificaciones que fueran posible, el siguiente paso, dentro del equipo Technology Governance Risk & Control era la valoración de cada uno de estos procesos y subprocesos. Significaba darle no solo un valor monetario sino el valor sustancial fuera de lo material que le atribuía la organización.

Para ello debíamos asumir que un proceso tiene un beneficio o costo financiero fácilmente medible, y también un beneficio o costo no financiero un tanto más difícil de mensurar.

¿Qué es un beneficio comercial?

El beneficio comercial se puede definir como el resultado de una acción o decisión que contribuye a cumplir los objetivos comerciales.

Esa definición sirve para muchas necesidades de planificación empresarial y análisis comercial. La definición de beneficios comerciales en términos de objetivos comerciales proporciona una base práctica para medir, valorar y comparar los beneficios financieros y no financieros.

Beneficios financieros vs. no financieros:

- El concepto de beneficio comercial es central en la planificación estratégica y en la mayoría de las formas de análisis de casos de negocios, donde se evalúan las acciones en términos de los posibles resultados de costos y beneficios. Aquellos que persiguen estas actividades aprenden rápidamente, sin embargo, que algunos tipos de beneficios son más fáciles de medir y valorar que otros.

- La mayoría de las organizaciones aceptan fácilmente los resultados financieros positivos como beneficios comerciales. Estos son fáciles de medir en términos de ahorro de costos, crecimiento de los ingresos, entradas de efectivo o mayores ganancias.
- Muchas personas, sin embargo, no están seguras acerca de cómo medir o valorar las contribuciones a los objetivos comerciales que definen en términos no financieros. Estos pueden incluir, por ejemplo, cambios en los indicadores clave de rendimiento para los objetivos que tienen que ver con:
    - ✓ La satisfacción del cliente.
    - ✓ Compromiso de los empleados.
    - ✓ La reducción de riesgos.
    - ✓ Marca.
    - ✓ Calidad de entrega de producto.
    - ✓ Imagen de la empresa.

Se puede observar aquí, que prácticamente todos los factores enunciados anteriormente reúnen las características del Plan **TGRC**, demostrando una vez más lo agresivo y ambicioso de los objetivos.

Beneficios no financieros:

El principal escollo en las reuniones con los encargados, principalmente de producción, lo constituía la comprensión del tipo de beneficio no financiero donde seguramente todos los que formaban parte de la organización podían aportar poco o mucho, pero siempre aportar. En otras palabras, no consideraban automáticamente todas las reclamaciones de beneficios como legítimas. Esto es especialmente cierto para las contribuciones a objetivos no financieros, que se miden indirectamente a través de indicadores clave de desempeño.

Por ejemplo, si el análisis espera ahorros de costos bajo un plan de propuesta, la mayoría de las personas aceptan los ahorros como un beneficio "legítimo". Sin embargo, si el analista muestra un beneficio de $ 5 millones derivado de algo así como una mayor satisfacción del cliente o una mejor imagen de la empresa, probablemente no todos otorguen automáticamente al beneficio la misma legitimidad.

La última descripción se constituye en un principio inalienable dentro de la organización: todos somos parte del cambio y contribuimos a llevar a la organización a ser líder en cada uno de los segmentos que participa.

Luego, en el capítulo destinado al Plan de Gestión de Contingencia (Resiliency Management Plan) se abordará nuevamente el tema de la identificación de procesos.

6 COORDINAR LAS ACTIVIDADES

6.1 Coordinar y su Implicancia en Proyectos

Los coordinadores de proyectos generalmente trabajan bajo la dirección de un gerente de proyecto para ayudar con tareas administrativas en un proyecto específico. Básicamente ayudan a garantizar que todos los miembros y departamentos del equipo tengan lo que necesitan para cumplir con los plazos e hitos establecidos por el gerente del proyecto. Para ello, también deben estar familiarizados con todos los aspectos del plan de despliegue, incluidos todos los períodos cortos y largos, objetivos a largo plazo, todo el calendario del proyecto y detalles del presupuesto.

Mientras que los gerentes de proyecto supervisan todo el proceso desde la planificación hasta la finalización, el rol del coordinador del proyecto está más centrado en la ejecución de etapas específicas de un plan. El objetivo del coordinador del proyecto es ayudar a que el administrador del proyecto se centre en cuestiones más amplias y en cualquier problema que pueda surgir al administrar las minucias cotidianas de un proyecto. En ocasiones, los coordinadores pueden eventualmente ampliar sus responsabilidades para incluir proyectos múltiples, o pasar a funciones de gestión de proyectos con más supervisión.

Todos estos roles fueron asumidos por el autor, incluso actividades de jerarquía más importante que coordinador, como por ejemplo auditor.

Además de las responsabilidades que se vienen mencionando a lo largo del presente trabajo, se podría definir el rol del autor para el proyecto **TGRC**, como el responsable de la ejecución del proyecto para Beef Argentina siendo el nexo entre el Gerente Global de TGRC en Mineapolis y las dos plantas (Nelson y Bernal) que constituían la Unidad de Negocios.

6.2 Coordinar las Actividades de Riesgo y Control

La esencia del Proyecto de Gobierno y Control de los Riesgos Tecnológicos (**TGRC**), es asistir a la plataforma de la empresa y el Centro de Servicios Compartidos (SSC) a incorporar conceptos, herramientas y conocimientos para procurar proteger los derechos intelectuales y mantener el nivel de confianza depositado en la empresa por los clientes. Lo definido anteriormente, es el concepto asociado a "reputación" frente al mundo. Una empresa cuya Base de Datos es vulnerada y los datos de los clientes -seguro social, número de cuenta bancaria y otros datos confidenciales- son accedidos por personas no autorizadas, se verá muy afectada en cuanto a su imagen, reputación y confianza no solo de sus clientes sino también sus inversores.

En cuanto al cumplimiento de las políticas y métricas establecidas o definidas por **TGRC**, así como lograr que las mismas sean entregadas y accedidas por el personal involucrado, el equipo define nuevos roles dentro de la Plataforma que son requeridos en la etapa de coordinación.

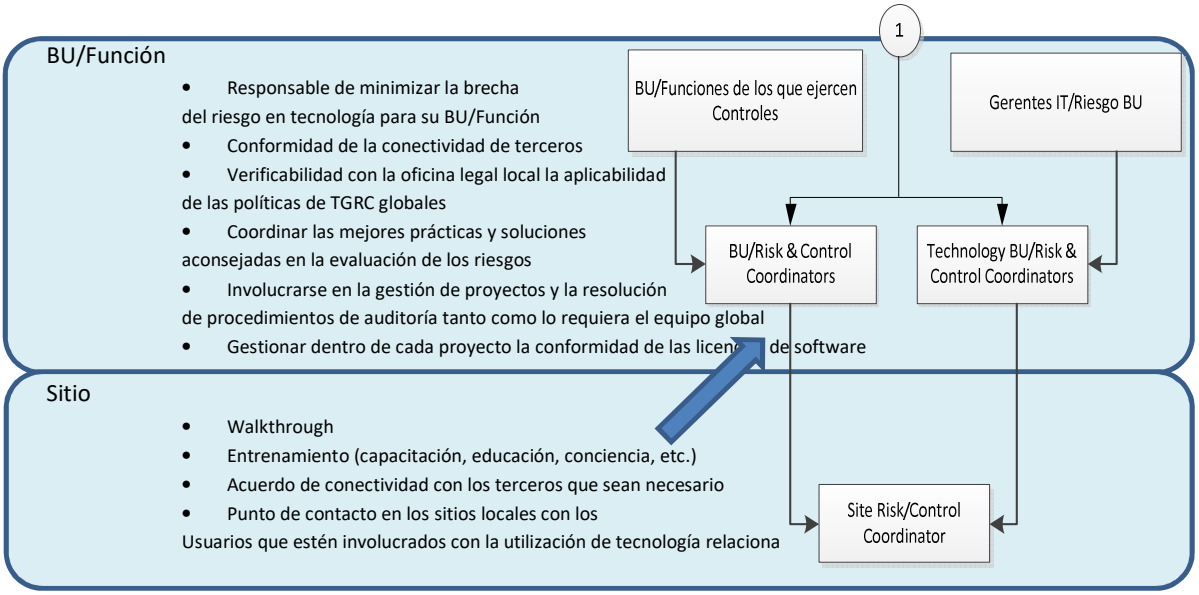


Figura 14. Nuevos roles para direcciones de las políticas entregables del Centro de Coordinación de Riesgos (RCC).

Uno de aquellos roles (indicado por la flecha el lugar donde se adicionará) es el Coordinador de Riesgo y Control (RCC).

Los objetivos Primarios del RCC son:

- Coordinar y asegurar que todos los sitios dentro de las funciones y negocios dentro de la empresa tienen identificados los coordinadores de riesgo y controles dentro del lugar en cuestión.
- Asegurar que todo lo definido anteriormente haya sido informado de la mejor manera y entrenado por alguno de los métodos utilizado por la organización.
- Es requerido un monitoreo fehaciente para completar las caminatas de control (walkthrough) y supervisión para todos los sitios donde fueron asignados los responsables.
- Coordinar y asegurar que todos los mensajes de **TGRC** y sus Unidades de Negocios/Funcionales sobre la generación de conocimiento, han sido entregados de la manera más apropiada en el tiempo conveniente a todos los coordinadores de riesgo y control en el mundo.
- Coordinar y asistir a los controladores a nivel mundial en lo que es traducción de una forma correcta para evitar errores en la transmisión y educación del conocimiento en las Unidades de Negocios/Funcionales.
- Coordinar y revisar la actualización del Análisis de Impacto de Negocios (BIA) para las correspondientes Unidades de Negocios/Funcionales de acuerdo a las métricas elaboradas en función de los objetivos fijados.
- Asistir a la Unidad de Negocio correspondiente, en el conocimiento de la "brújula de soluciones". Traducción más apropiada dada por los americanos para referenciar el término original SecurCompass, que implicaba el conocimiento -ante una situación de anormal o de emergencia- de todos los procesos definidos para el caso, como así también los responsables. No será desarrollado en el presente trabajo, pero la organización destinaba un grupo, herramienta web, entrenamiento y material sólo para SecurCompass. Surge como consecuencia que muchas organizaciones en el mundo para las cuales sus empleados no saben cómo actuar o a quien dirigirse ante una situación anormal o de emergencia.

6.3 Principales Áreas de Riesgo (KRAs)

Los Indicadores Clave de Riesgo (KRI[25]) son predictores críticos de eventos desfavorables que pueden tener un impacto adverso en las organizaciones. Controlan los cambios en los niveles de exposición al riesgo y contribuyen a los primeros signos de advertencia que permiten a las organizaciones informar los riesgos, prevenir crisis y mitigarlas a tiempo.

Todos esta evaluación y establecimiento de los indicadores necesita una definición correcta de los procesos existentes dentro de la organización. Etapa que ha sido tratada en el capítulo anterior, intentando el autor mantener una coherencia en el marco de todas las actividades y responsabilidades desplegadas en la compañía.

Los KRI, independientemente o en conjunto con otros datos relacionados con el entorno de riesgo, como eventos de pérdida, resultados de evaluación y problemas, ofrecen una comprensión considerable de las debilidades dentro de los entornos de riesgo y control. Actúan como métricas de los cambios en el perfil de riesgo de una organización, pero dado el cambiante panorama de los riesgos, simplemente establecerlos dentro del protocolo corporativo puede no ser suficiente.

Estos KRI nos aportarán una gran herramienta para elaborar una escala de las áreas cuyos indicadores resulten más elevados correspondiendo a las Principales Áreas de Riesgo o (KRA[26]).

6.4 Encontrar las Principales Áreas de Riesgo (KRAs) Dentro de la Empresa

En el trabajo del equipo **TGRC**, se definía un conjunto de indicadores que permitían establecer o encontrar las Principales Áreas de Riesgo, cuyos procesos han sido identificados y se les ha asignado un KRI que indicaba su índice de criticidad. Estas KRAs debían tener un plus de supervisión y seguimiento en lo que respecta a gestión y cumplimiento de las políticas definidas dentro de la empresa.

Los dos principales patrones de riesgo que mantenían una estrecha vinculación con el equipo de Gobierno y Control de los Riesgos Tecnológicos eran:

- **Categoría de Riesgo 1**: ***Antimonopolio y Corrupción***. Estos riesgos están regulados por leyes en todo el mundo. La intención de estas leyes es garantizar que las empresas realicen negocios de manera ética, promuevan la

[25] Key Risk Indicator
[26] Key Risk Area

competencia leal en beneficio de los consumidores y prohíban el comportamiento deshonesto de las personas confiadas en un puesto de autoridad.

- ***CORRUPCIÓN Y SOBORNO.*** El soborno y la corrupción a terceros es un área de riesgo creciente para cualquier empresa que realice negocios a nivel internacional como la empresa de estudio. La Ley de Prácticas Corruptas en el Extranjero de los Estados Unidos, la Ley contra el Soborno del Reino Unido y muchas otras leyes en todo el mundo obligan a las empresas a tomar medidas para garantizar que sus terceros no se involucren en prácticas corruptas. Dentro de los principios guías en la empresa, se encontraba un apartado especial dedicado al tema regulación.
- ***SANCIONES Y EXCLUSIONES.*** En aquellos días, *las* sanciones se usan tanto como "espadas" o como "escudos". Están siendo utilizados por los gobiernos con fines políticos y para imponer restricciones comerciales a empresas y personas. Se ha visto esto en las sanciones impuestas contra Rusia por los Estados Unidos y el gobierno europeo.
- ***FRAUDE, LAVADO DE ACTIVOS E IRREGULARIDADES FINANCIERAS***. Las leyes contra el lavado de dinero reflejan un esfuerzo realizado por los gobiernos para detener los métodos de lavado de dinero que involucran a las instituciones financieras. Según las pautas establecidas por el anti-lavado de dinero (o AML, por sus siglas en inglés), las instituciones financieras deben verificar todas las grandes sumas de dinero que procesan, y deben informar las transacciones sospechosas. Por ello, el equipo **TGRC** establecía aquí otra particular supervisión de la información financiera.

- **Categoría de Riesgo 2:** ***Ciber-seguridad y Estabilidad de los Negocios***. Un área con creciente atención de medios y preocupación por parte de la organización, es la ciberseguridad y la estabilidad comercial. El potencial de daño por el mal manejo de los datos de la compañía, del cliente y del producto puede causar daños irreparables a una organización. Además, las expectativas de salvaguardar la información de los consumidores están en su punto más alto de todos los tiempos.
  - ***INFORMACIÓN PERSONAL MAL MANIPULADA.*** El manejo de información privada identificable conlleva una gran obligación, tanto en virtud de la ley como también de acuerdo con las políticas de la compañía. Además, las expectativas de los clientes y proveedores a lo largo del mundo son muy altas: esperan que las empresas protejan su

información y la mantengan confidencial, no sea pirateada, hecha pública, entregada a terceros con fines de mercadotecnia o vendida al mejor postor.

- ***INCUMPLIMIENTOS EN LA SEGURIDAD DE LOS DATOS***. Al contratar a terceros (o dentro de la propia compañía), es muy probable que algunos obtengan información sobre la organización, productos, precios, empleados o clientes, y almacenen esa información en sus sistemas. La forma en que los terceros -o la empresa- almacenan su información, la tecnología utilizada para garantizar que siga siendo segura y confidencial, y la forma en que se intercambia la información con todos, debe ser evaluada y administrada de cerca. Como muchos terceros en estos días involucran soluciones tecnológicas (muchas de las cuales son soluciones alojadas), existe la necesidad de garantizar que los terceros tomen precauciones adicionales.
- ***CONTINUIDAD EMPRESARIAL.*** Los desastres naturales, los accidentes, la pérdida de información, las huelgas laborales y otras posibles interrupciones pueden detener o ralentizar inesperadamente el suministro de materiales que respaldan la fabricación de sus productos, así como el normal desarrollo de los procesos de la empresa. Comprender dónde la exposición potencial a la interrupción del suministro o producción y el desarrollo de planes de continuidad puede salvar a la empresa de la pérdida de ingresos y / o la erosión de la marca.
- ***INFRACCIÓN DE LA PROPIEDAD INTELECTUAL.*** La propiedad intelectual generalmente se describe como patentes, secretos comerciales, diseños, marcas comerciales y derechos de autor. Con el despliegue de procedimientos dentro de **TGRC** se aseguraba que la compañía no tenga, por ejemplo, ningún software que no sea original y que cada uno de los productos instalados en las computadoras que poseía en todo el mundo contaban con registro, número de serie, etcétera.

6.7 Relaciones Entre la Actividad RCC y las KRAs

El equipo de **TGRC** había definido perfectamente las actividades del grupo de coordinadores o actividades de coordinación y la Principal Área de Riesgo (KRA) asociada.

Los Analistas de Riesgo, otra responsabilidad asumida por el autor, basaban su estudio en la siguiente relación.

ACTIVIDAD	KRA
Participar en la revisión y aprobación de las guías de entrenamiento en la coordinación del control de riesgos	Anualmente revisar RCC las guías de entrenamiento.
Seguimiento en el llenado de los informes sobre caminatas de control (walkthrough), tanto como se requiera (mínimo trimestralmente) para todos los sitios donde haya un analista responsable, o sea: en todos.	Es requerido un reporte 100% completo e informado para cada Unidad de Negocios (trimestralmente mínimo).
Coordinar y asegurar que TGRC y las Unidades de Negocio/Funciones, se alinean a los mensajes distribuido en tiempo y forma, por los coordinadores de riesgo y control.	100% de todo el material desplegado sobre conocimiento o política a todos los empleados y contratistas en la Unidad de Negocio es requerido, al menos, trimestralmente (mensualmente supera).
Coordinar y asistir en la traducción del material para que el mensaje del esquipo TGRC llegue de manera correcta a quien involucra y evitar errores de traducción que afecten la educación en la Unidad de Negocio.	Identificar un traductor para el lenguaje nativo correspondiente a la Unidad de Negocio.
Coordinar la revisión y actualización del Análisis de Impacto de Negocios (BIA) para la Unidad de Negocio/Función del Analista.	100% del BIA completo para la Unidad de Negocio, como ha sido definido por TGRC Central.

Tabla 10. Relación Actividad – KRA para RCC.

Se puede comprender, al citar el último punto de la tabla, que esa actividad definida con esa simpleza no hace otra cosa que definir todo lo enunciado anteriormente (procesos, herramienta de software, evaluación, criticidad, etc.).

En cuanto a la forma de realizar el BIA, el autor considera oportuno definirla en el siguiente capítulo, como parte del Plan de Contingencias (Resiliency Management).

6.8 Identificación y Entrenamiento de los Coordinadores de Riesgo y Control en la BU/Función

Corresponde, dentro del plan central desplegado por Mineapolis, a los coordinadores de riesgos y control asistir a los controladores de la unidad de Negocios donde es

responsable. Además, identificar el Sitio de los Coordinadores de Control y Riesgo (SRCC). El coordinador de control de riesgo (RCC) es responsable por implementar las medidas correspondientes de seguridad para que el SRCC esté entrenado y pueda acceder a la plataforma web donde el material está disponible, considerando que solamente el SRCC puede acceder al material citado.

Es conveniente resaltar la importancia que le brindaba **TGRC** a lo que eran permisos de acceso como parte de un programa general de control de riesgos. En ciertas Unidades de Negocio, el SRCC podía cubrir múltiples locaciones en la coordinación de las expectativas de **TGRC,** aun así, no significaba un impacto en detrimento de su responsabilidad.

Se destaca la importancia de elaborar la lista inicial de SRCC y cualquier cambio subsecuente que necesite ser rápidamente comunicado al gerente de la Plataforma de Control de los Riesgos Tecnológicos y etiquetado de los Analistas de Control de los Riesgos Tecnológicos. Una etiqueta incluía todos los datos del analista, desde su nombre de sesión, contraseña o visualización hasta sus permisos de utilización, acceso o modificación de los datos.

Como en los casos mencionados en puntos anteriores, se desarrolló las funciones descriptas al asumir el rol de Responsable Beef Argentina cubriendo las locaciones de Bernal en Buenos Aires y Nelson en Santa Fe.

6.9 Coordinación del Entrenamiento de los Usuarios

El objetivo de los programas de conocimiento y entrenamiento de los usuarios en la utilización de las tecnologías, es asegurar que cada uno de ellos es consiente y comprende sus obligaciones y como ellos son máximos responsables en la protección de la información crítica además de la mitigación de los riesgos tecnológicos.

- ✓ El RCC era responsable de ***desplegar***, a modo de entrenamiento, el conocimiento sobre la tecnología usada dentro de la Unidad de Negocios.
- ✓ En los lugares donde las Unidades de Negocio se encontraban en un país donde el inglés no era su lengua materna, la ***traducción*** y entrega del material en tiempo y forma era una función más del RCC, tal como se referenció anteriormente.

Despliegue y traducción del conocimiento:

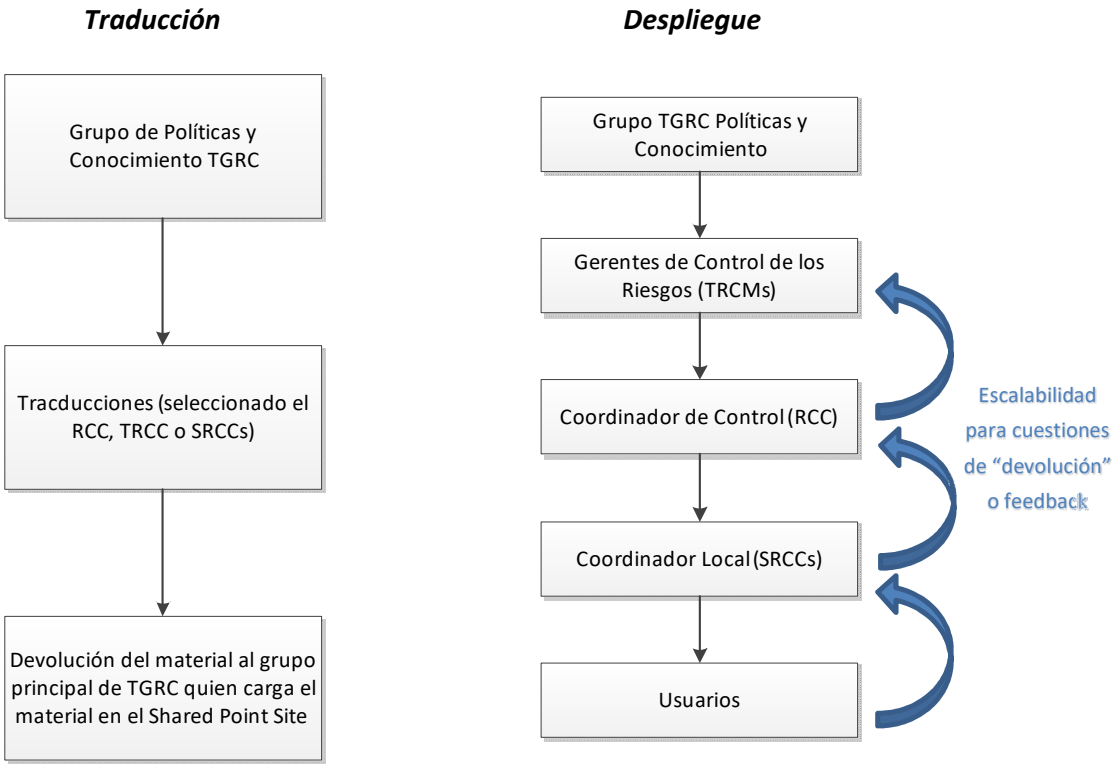


Figura 15. Traducción y Despliegue de conocimientos.

El equipo **TGRC** estaba estructurado de manera tal que SRCCs puede, y debería, escalar a su TRCCs las cuestiones que podrían ser más técnicas o requieren de un tecnicismo más importante.

6.10 Coordinación de las Caminatas de Control o WALKTHROUGH

Las caminatas de control o walkthrough, era un método que la empresa utilizaba para reducir los riesgos y, desde luego, esperaba compromiso de todos sus empleados. Las caminatas se efectuaban en todas las oficinas sin importar el cargo, escritorios y lugares de trabajo para el chequeo y supervisión del resguardo correcto de contraseñas y documentos confidenciales, habilitación de pantallas de bloqueo (screensavers) con contraseña a partir de los 5 minutos de reposo del equipo y muchos otros requerimientos más. Una hoja suelta dejada en un escritorio deberá ser evaluada si constituye o no un riesgo (números de teléfono, cuentas, dirección, seguro entre otros). Se generará una nota con las violaciones a las políticas de la empresa, el

causante y algún otro dato relevante; luego se cargará el resultado de la caminata en una base de datos. Para el escritorio había una política denominada *escritorio limpio*, indicando que no podía haber ninguna información confidencial al alcance de personas no autorizadas.

Luego, eran generados los reportes y distribuidos incluyendo el nombre de aquellos empleados que quebrantaron las normas de la empresa. El equipo tenía total apoyo para informar tanto a un operador de un puesto productivo como a un gerente de planta lo que evita futuras sanciones.

7 COORDINACIÓN DE RIESGOS PURAMENTE TECNOLÓGICOS

7.1 Coordinar las Actividades de Control de Riesgos Específicamente Tecnológicos

El área donde se adicionan las funciones se puede observar incorporando nuevamente el grafico visto anteriormente.

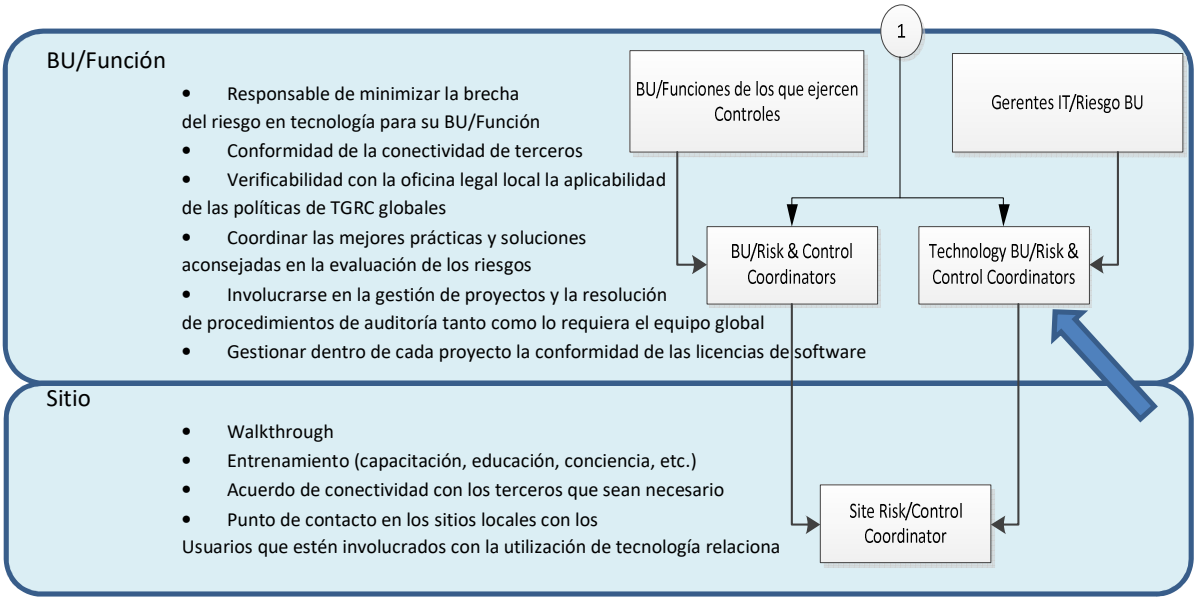


Figura 16. Nuevos roles TRCC para direcciones de las políticas de TGRC.

Uno de aquellos roles (indicado por la flecha el lugar donde se asume la responsabilidad), es el Coordinador de Control y Riesgos Tecnológicos (TRCC). El objetivo primario de este rol es involucrar el conocimiento y la coordinación de la actividad de los procesos de mitigación de los riesgos tecnológicos.

Lo que resta del presente capítulo, se describen los procesos y las herramientas para que el rol tenga un correcto despliegue.

Un bosquejo del detalle de las KRAs para éste nuevo rol, es expuesto en la siguiente sección.

7.2 Relación Entre la Actividad TRCC y las KRAs

El propósito de las KRAs para este rol, es reportado en la tabla:

ACTIVIDAD	KRA
Coordinar y asegurar que los bienes tecnológicos son administrados alineados a las políticas de la empresa.	100% de la tecnología que es desechada, donada o retirada por cualquier motivo, se ajusta a los procesos/servicios aprobados (ej: limpieza 100% de todos los discos rígidos). 100% del nuevo software sigue los requerimientos de los procesos SAM. Tendencia a la baja del número de licencias de software requeridos. 100% de las licencias del software han sido debidamente comprobadas y guardadas en la herramienta apropiada.
Revisar el cumplimiento de los reportes y asegurar que la acción apropiada es tomada para llevar a la BU a la satisfacción de la política si fuera necesario (ej: planes de acción de vulnerabilidad, redes compartidas, etc.)	Para el caso de no poseer licencia para un software requerido. Tendencia a la baja de políticas no cumplidas. 100% de “verde” en la escala de cumplimiento de parches.
Coordinar la revisión, aprobación y prueba del Plan de Recuperación de Desastres usado como entrada para el Análisis de Impacto de Negocio correspondiente.	Basado en los requerimientos del BIA, despliegue prueba y mantenimiento del 100% de los planes de recuperación para las BU.
Coordinar y asegurar que todas las etiquetas de políticas tienen sustituto y los controles de compensación han sido definido.	Aplica a todas las áreas que posean procesos que dependan de tecnología activa.

Coordinar la completa evaluación de los riesgos tanto como exija TGRC (ej: Aplicaciones, Proveedor de Servicios de Aplicaciones, etc.).	Es requerida la evaluación de aquellas aplicaciones que fueran críticas (que han sido identificadas por el BIA). 100% de todas las aplicaciones.

Tabla 11. Relación Actividad – KRA para TRCC.

7.3 Coordinación en Parches de Seguridad y Antivirus

Ciertas exigencias del **TGRC** podían ser satisfecha en un determinado tiempo, por ejemplo, el Análisis de Impacto de Negocio en el cual se evaluaba su proceso de crecimiento o expansión porque eran parte de un proyecto a 2 o 5 años.

En el caso de los parches, se exigía el cumplimiento mensual porque de ello dependía la seguridad de la información en toda la empresa, quien usaba la frase "una cadena es tan fuerte como su eslabón más débil". Por lo tanto, una computadora con los parches desactualizados o deficiencias en la seguridad era un punto de acceso de intrusos, ya sea a software malicioso o simplemente un empleado descontento.

La actividad exigía coordinación mundial. Dos medidas de seguridad eran implementadas por Servicios de Negocio IT (ITSB): IT Planta y otras áreas de IT administradas para la Unidad de Negocio donde haya dispositivos que le sean aplicables parches de seguridad e instalable software antivirus. A pesar de que para los dispositivos administrados o supervisados por ITSB, el grupo es responsable de la instalación de parches de seguridad y el despliegue del antivirus, se espera la Plataforma asegure también el cumplimiento de los mismos y no se desligue de las responsabilidades.

En cuanto al seguimiento del despliegue de parches de seguridad y software antivirus en las computadoras del mundo, mediciones de cumplimiento o satisfacción son creadas e incorporadas en el reporte mensual de **TGRC** denominado *scorecard*, y que se ha tratado anteriormente.

7.4 Tablero de Control o Scorecard de TGRC y su Rol en la Coordinación

El *scorecard* tiene un rol muy importante en la coordinación de las actividades para poder alcanzar las metas fijadas por la empresa en íntima relación a los riesgos tecnológicos.

En la organización central de **TGRC**, cada mes, el tablero de control es creado. Una herramienta basada en Excel es también actualizada, permitiendo a los responsables identificar cuales dispositivos no están en conformidad a los objetivos o normas que componen los lineamientos en las políticas de la empresa en lo que respecta a parches de seguridad y software de antivirus. El *scorecard* es utilizado para "perforar" la organización, incluyendo todas sus locaciones específicas y departamentos, en la búsqueda de dispositivos que requieran un seguimiento especial para asegurar se cumplan las normas de seguridad exigidas.

Cada Plataforma/Función de Analistas de Riesgos Tecnológicos (TRA) o Gerentes de Control y Riesgos Tecnológicos (TRCM) tendrá a su disponibilidad los reportes o la información con el tiempo previsto -una semana- antes de cada reunión mundial para revisar la conformidad o no cumplimiento de las métricas.

7.5 Coordinación en la Evaluación del Software

El rol de la coordinación en la evaluación del software, lo desempeña el Coordinador de Control y Riesgos Tecnológico (TRCC), quien refleja en un sitio de acceso mundial, todos lineamientos, actualizaciones o modificaciones de los requerimientos a ser satisfechos por Plataforma Global.

El objetivo primario y esencial de la actividad de desplegar una evaluación de las aplicaciones, es identificar las áreas con oportunidad de mejoras en la seguridad dentro de la organización en su concepción mundial. Cuando se evalúa una aplicación, cualquier factor puede, y necesita, ser considerado: accesos lógicos, no conformidad de políticas, varianzas, consideraciones del marco tecnológico, acuerdo de soporte, etcétera.

Cada Plataforma con su correspondiente TRA y el TRCM determinará cual sería la mejor aplicación usada para una situación específica. La necesidad de nuevas aplicaciones es permanente en cada Plataforma de Negocio/Función debido a nuevos requerimientos, clientes y regulaciones gubernamentales solo por mencionar algunos. Obviamente, después de una reingeniería de procesos es probable necesitar nuevas aplicaciones que no estarán disponibles hasta no ser autorizadas por **TGRC**, aunque peligre el nuevo proceso o negocio.

7.6 Coordinación en la Revisión de los Accesos Lógicos

Actividad por demás importante dentro del grupo, de los accesos depende también la seguridad de la información no solo de producción sino contable, de empleados, clientes, proveedores, estado de procesos, etcétera.

Los datos son considerados unos de los activos importante dentro de la corporación. Se mencionó anteriormente, es un área de énfasis el control de los accesos lógicos dentro de la empresa a la información. Las políticas completas sobre protección y acceso a la información son almacenadas en **ARCHER** para conformar el Centro de Políticas, calando en lo más profundo del área de acceso lógico al recurso.

Figura 17. Centro de Gestión de amenazas en Archer.

Lo arriba mencionado, constituye el Centro de Gestión de Amenazas núcleo del Centro de Políticas para proteger la información como recurso activo y vulnerable.

El *scorecard* utilizado como herramienta para la coordinación de las actividades, también posee una sección destinada al acceso lógico y se puede apreciar en la parte inferior la siguiente figura. En ella se observa los puntos de control definidos para el Control de Acceso, como también los procesos de documentación requeridos por **TGRC**.

Service Unit Metrics - Report Period May 2011		BU EUROPE	SU-BEFF Argentina
	# of Applications in Inventory (Total: 354)	25	50
Business Impact Analysis		100%	100%
	Application-based BIA Completed	100%	100%
	Application-based BIA Updated or Created in the Last Year	100%	100%
Disaster Recovery		**100%**	**81%**
	DR Requirements - # of Applications	4	4
	Has DR Plan	100%	75%
	DR Plan Implemented	100%	75%
	DR Plan Tested	100%	75%
	DR Test Conducted in the Last Year	100%	100%
Information Access Controls		**91%**	**100%**
	Doc. Proc. For User Administration	64%	100%
	Doc. Proc. For Approving Access Requests	96%	100%
	Doc. Proc. For Immediate Removal	96%	100%
	Doc. Proc. For Access Change Notification	100%	100%
	Doc. Proc. For Monitoring	96%	100%
	Doc. Proc. For User Access Reviews Every 12 Months	100%	100%
	Access Review conducted in the last year	**100%**	**100%**
	Documented Training Plan	80%	100%
	Periodic Review of Roles and Responsibilities	80%	100%
	Review of roles and responsibilities conducted in the last year	**100%**	**100%**

Tabla 12. Informe de Archer utilizado como coordinación.

El puntaje del *scorecard* representado en los diferentes promedios para cada ítem, se muestra en la siguiente figura.

Key:			
Business Impact Analysis	<80%	80% - 90%	> 90%
Disaster Recovery	<80%	80% - 90%	> 90%
Information Access Controls	< 70%	70% - 99%	>99%

Tabla 13. Calificación utilizada.

Toda aplicación que posea la empresa, se espera tenga creada la documentación y posea el registro en **ARCHER** sobre el acceso lógico a la misma. Las siguientes, son preguntas que requieren ser respondidas:

- Siguen los accesos a la aplicación un proceso de documentación para los permisos de usuario a las vistas, modificación y eliminado de datos?
- Siguen los accesos a la aplicación un proceso de documentación para aprobar/autorizar el acceso a un recurso requerido?
- Siguen los accesos a la aplicación un proceso de documentación para la inmediata remoción de permisos de acceso? Por ejemplo, al despedirse un usuario.
- Sigue el acceso a la aplicación un proceso de monitorización periódico de utilización?

- Ha seguido el acceso a la aplicación un proceso para la revisión de los permisos por parte del administrador o los propietarios de sistema (owner, en el caso de delegación de responsabilidad) durante los últimos 12 meses?
- Ha seguido el acceso a la aplicación un plan documentado de entrenamiento en la utilización del recurso?
- Son los roles y responsabilidades, para la gestión segura de la información, revisados y actualizados periódicamente?

Solo algunas de las tantas cuestiones que requerían ser respondidas en el marco de una gestión de los riesgos de manera responsable.

7.7 Coordinación de Ciclo de Vida del Hardware

Un rol no menos importante en lo que respecta a la actividad de coordinación, era la del ciclo de vida del hardware. La empresa contenía, y de hecho contiene, aunque el autor no pertenezca en la actualidad, información sobre todo el hardware y software activo identificado. Ello se embebía y documentaba dentro de los Documentos KRA.

El conjunto de información contenida conformaba lo que se conocía bajo el nombre de Política de Protección de la Información Activa. Por lo tanto, hace al ciclo de vida del hardware o software -desde su adquisición hasta su deshecho- convertirse en un punto crítico de control de la información activa en la organización.

Por ejemplo, era común que luego de tres años los equipos (eran todos Dell) se comiencen a donar a entidades, organizaciones y escuelas, logrando una participación muy importante en la colaboración del progreso de la comunidad donde opera. Un proceso extremadamente importante en la donación era la política denominada DISPOSAL, en ella se eliminaba cualquier información del equipo relativa a la empresa cumpliendo con las normas definidas por **TGRC** y disminuyendo el riesgo de accesibilidad datos activos.

7.8 Coordinación en los Acuerdo de Acceso a la Red (NAA[27]) y Evaluación del Riesgo (NCRA[28])

La coordinación de los NAA es una “legalidad” o norma entre la empresa y aquellos terceros prestadores de servicio o clientes, es decir, cualquier organización con que se mantenga relación y necesite acceso en cierta escala a la información. Esta conexión entre la red de la empresa y otra red ajena, debe estar documentada y aprobada en lo

[27] Network Access Agreements
[28] Network Connectivity Risk Assessment

denominado Documento de Seguridad de Red el cuál no puede ser obviado ni por una Unidad de Negocio ni por la casa central.

Cada vez que la empresa participa en una fusión (Cargill-CHS), adquisición (Finexcor-Cargill) o proyecto conjunto, debe incluir un plan de ambientación siendo una de las primeras actividades la necesidad de conectarse, es decir, compartir datos e información mediante algún tipo de enlace de ambas redes.

Ejecutar un plan NCRA implica identificar riesgos, acciones necesarias y aprobar requerimientos, tan pronto como sea posible. Conectar las redes debe tener un potencial nivel de riesgo aceptable y manejable. Si excede lo aceptable, entonces hará caer el negocio. ***Algo que todo Ingeniero en Sistemas debe considerar: la seguridad no tiene precio ni tampoco se negocia…con nadie.***

8 PLAN DE CONTINGENCIAS o RESILIENCY MANAGEMENT PLAN

8.1 La Necesidad de un Plan de Contingencias en la Empresa

Los constantes cambios de los requerimientos en las Unidades de Negocio que la empresa tiene desplegados en el mundo han impulsado la evolución de las primeras soluciones de recuperación con plazos de días a semanas para el entorno actual en la exigencia de continuidad para las operaciones de negocios y IT. Donde la recuperación de desastres una vez dio paso a la continuidad del negocio a mediados de la década de 1990, la continuidad del negocio ahora está dando paso a la capacidad de recuperación de los negocios. Las técnicas de disponibilidad, recuperación, seguridad y cumplimiento han convergido y deben ser administradas al mismo tiempo para crear una infraestructura que pueda sostener la resiliencia empresarial real. Es la convergencia de estas técnicas dentro de un entorno altamente seguro que obliga a los gerentes de resiliencia de negocios a administrar elementos más complejos al mismo tiempo y en proporción al nivel de servicio que demanda la empresa.

Para lograr este objetivo, alcanzar además la certificación internacional que lo exige, la empresa desarrolló un programa integral y multifuncional orientado a mantener las operaciones comerciales continuas y el acceso a los datos comerciales críticos, mientras se administran, gestionan y predicen los costos para mantener y mejorar un estado altamente preparado de la organización frente a contingencias. La capacidad de combinar soluciones para dar cabida a los procesos -definidos anteriormente- y las aplicaciones empresariales más críticas con soluciones no tan estrictas -esto es “sigamos operando”- es una marca registrada de la empresa *resistente*.

Una de las razones por la que anteriormente definimos procesos, es la relación con la resiliencia o hacer frente a contingencias. La gestión de la resiliencia significa una gestión integral de los procesos para ayudar a identificar los riesgos potenciales en función de los impactos que amenazan a la empresa. Su aspecto más crítico, lograr un sólido Plan de Gestión Contingencias o Resiliency Management para ayudar a la empresa a adaptarse y responder más rápidamente a los riesgos y oportunidades para mantener las operaciones comerciales en forma continua, ser un socio confiable y permitir crecimiento, aún en situaciones de crisis.

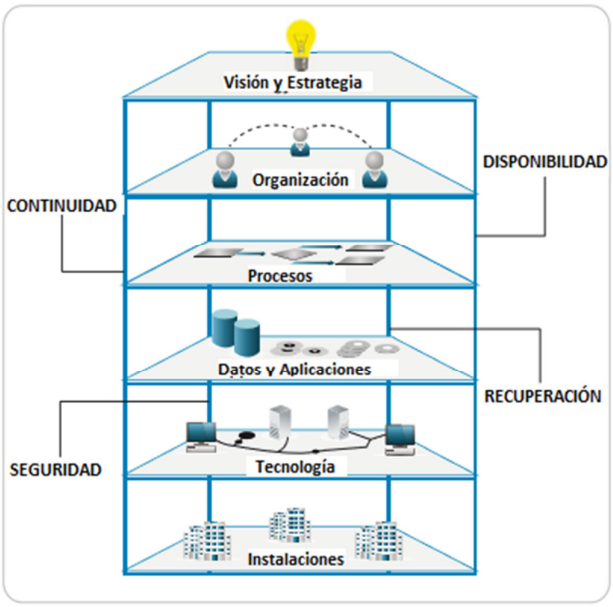


Figura 18. Marco de Resiliencia de la Unidad de Negocio

En el marco expuesto anteriormente, dentro de la organización los Ingenieros y Analistas procedieron a desplegar un plan que significaba uno de los puntos más importantes y relevantes del trabajo del autor en la Unidad de Negocios Beef Argentina. Plan demandante no solo de una gran coordinación, sino también, una inmensa cooperación y trabajo en equipo; se debe tener presente que el plan era implementado y evaluado a nivel mundial. En la empresa de referencia, el trabajo en equipo se consideraba una habilidad y aptitud tan importante que formaba parte del Plan de Desarrollo Personal que determinaba los incrementos salariales anuales y cuya conformidad o alineación a los objetivos era revisada semestralmente, de modo tal que la evolución no solo era observada por el gerente directo, la supervisión incluía

líderes de Mineapolis. Obviamente, no en todos los sectores o puestos sino en la actividad desarrollada por el autor.

Siempre acudiendo a esas frases duras y ciertas, el equipo debía tener presente el concepto expuesto en las reuniones:

"Más que educación, más que experiencia, más que entrenamiento, el nivel de resistencia de una persona determinará quién tiene éxito y quién falla. Eso es cierto en la sala de cáncer, es cierto en los Juegos Olímpicos, y es cierto en la sala de juntas"

Ejemplificando de esta forma que el éxito de la empresa lo determinaba su resistencia a las contingencias. La resistencia significaba continuar operando y generando ingresos aún en situaciones de desastres o eventuales interrupciones de sus procesos principales. Ellos podían ser desde una destrucción de centro de datos por razones inesperadas, perdida del enlace satelital porque un camión retrocedió y embistió la antena, a todas las amenazas potenciales que pueden imaginarse.

Dentro de la corporación, el apoyo a planes de vanguardia en lo que respecta **TGRC**, surge de la importancia que poseía el cargo de Mrs R. Heise, Vicepresidente Corporativo y Jefa de la Oficina de Información de la compañía, quien se retiró en 2011 para iniciar en enero de 2012 su actividad como Consultora de Negocios.

8.2 Componentes del Plan de Gestión de Contingencias o Resiliency Management

Aplicación de la inteligencia de amenazas a los marcos de la resiliencia operativa y la gestión del riesgo, significa considerar, al aprovechar la inteligencia de amenazas que el profesional de resiliencia operacional no necesita crear un proceso competitivo independiente de otros marcos que la organización está aprovechando. De hecho, el uso de productos de inteligencia en la gestión de la resiliencia operativa no solo es compatible con muchos marcos existentes, sino que, en muchos casos, es inherente.

La consecuencia inmediata de lo expuesto fue definir un Plan de Gestión de Contingencias o Resiliency Management Plan, consistente y global, con su respectivo seguimiento de conformidad de los objetivos; compuesto por los cinco siguientes planes que, a su vez, eran requeridos:

- ***Análisis de Impacto de Negocios o Business Impact Analysis (BIA)***: Una evaluación de los procesos de negocio para determinar riesgos, mitigarlos y disponer de alternativas para que la empresa siga operando.

- ***Planificación de la Continuidad del Negocio o Business Continuity Planning (BCP)***: Los planes que aseguran una continuidad de las funciones y procesos críticos de negocio continúen operando o se mantengan sostenibles durante una interrupción importante (desastre, fuera de servicio de una aplicación importante, etc.).
- ***Planificación de la Recuperación de Desastres o Disaster Recovery Planning (DRP)***: el planeamiento y la preparación de IT necesarios para minimizar las pérdidas, asegurar la rápida recuperación de las aplicaciones críticas del negocio y continuar con el soporte de IT durante un desastre o contingencia que afecte a la empresa. Debería incluir planificación para la reanudación o recuperación de aplicaciones, datos, hardware, comunicaciones y otros aspectos de IT.
- ***Planificación de la Gestión de Crisis o Crisis Management Planning (CMP)***: el conjunto de acciones necesarias para tomar el control y comandar las actividades durante una interrupción. El proceso en el cual, una organización enfrenta de la mejor manera un evento que amenace con dañarla. La empresa posee un profundo sentido de pertenencia al entorno, considerando "daño" no solo a la propia organización sino también a sus proveedores, clientes o comunidad en general.
- ***Pruebas***: las pruebas del Plan de Gestión de Contingencias (RM) de acuerdo a las exigencias de las políticas corporativas.

En el capítulo 5 del presente trabajo, se abordó la importancia y necesidad de identificar procesos y subprocesos dentro de la organización. Ellos son el pilar fundamental de la reingeniería de procesos y base del Resiliency Management. Se desarrollará a continuación, principalmente, el BIA y BCP que permiten evaluar la situación y continuar operando.

8.3 Análisis de Impacto de Negocio o Business Impact Analysis (BIA)

Mensaje Principal de Necesitar un BIA:

El BIA es una evaluación que será usada para identificar los dos costos de referencia en el impacto: los costos financieros y no financieros. Los mismos, son pérdida durante el tiempo de interrupción que se produzca la contingencia.

Método Previo:

- Cada unidad de la empresa o función, completaba su BIA anualmente.

- El BIA se enfocaba su evaluación sobre aplicaciones.
- Contaba con dos indicadores de evaluación:
    - Obligaciones regulares.
    - Impacto financiero.
- No había un método formal consistente para desarrollar el BIA.
- El BIA no era gestionado o almacenado centralmente.

Método Actual:

- Cada unidad de la empresa o función, debe completar su BIA anualmente.
- El BIA enfoca su evaluación en procesos de negocios, tal como lo ha definido y exigido el Proyecto TARTAN.
- Se incluyen nuevos factores de evaluación:
    - Empleados
    - Resiliencia
    - Competitividad
    - Reputación
- Gestión central con la incorporación de una nueva herramienta, Archer:
    - Consistente
    - Aproximación formal
    - Centralizada
    - Reportes estandarizados
    - Procesos mensuales de supervisión de avances
    - Procesos anuales de revisiones para cada BU/Función

Objetivos y Principales Características del BIA:

El objetivo del BIA es ayudar a identificar las Unidades de Negocios, operaciones y procesos que son esenciales para la supervivencia de la BU o función. El Business Impact Analysis facilitará la identificación de cuán rápidamente deben estar operables las unidades de negocios y los procesos considerados esenciales luego de una interrupción; esto delineará el impacto en el negocio ante los escenarios de desastre sobre la capacidad de entregar productos o mantener los servicios de misión-critica. El BIA también ayudará a identificar en los planes ulteriores que recursos son requeridos para reanudar las operaciones de una BU a un nivel de “supervivencia” (BCP y DRP).

Lograr un acuerdo con la dirección ejecutiva sobre el tiempo crítico máximo que puede permanecer inoperable una actividad del negocio es fundamental a la hora de encarar el análisis de la BU y esto solo será posible si se ha identificado correctamente los expertos en la materia o ***subject matter expert.***

Los tres objetivos primarios del BIA son:

- Identificar los procesos críticos y priorizarlos de acuerdo a su criticidad.

- Evaluar el impacto de no contar con el proceso crítico funcionando.

- Estimar el tiempo objetivo de recuperación (RTO[29]) y el punto objetivo de recuperación (RPO[30]).

Consideremos ahora dos conceptos importantes que siempre debe tener en cuenta un Ingeniero en Sistemas cuando proceda a la definición de un Reciliency Management Plan.

RTO y RPO:

El punto objetivo de recuperación (RPO) y el tiempo objetivo de recuperación (RTO) constituyen dos de los parámetros más importantes de un plan de recuperación de desastres o protección de datos. Estos son objetivos que pueden guiar a las empresas a elegir un plan de respaldo de datos óptimo.

El RPO/RTO, junto con un análisis de impacto comercial, proporciona la base para identificar y analizar estrategias viables para su inclusión en el plan de continuidad del negocio. Las opciones de estrategias aplicables incluyen cualquiera que permita la reanudación de un proceso comercial en un marco de objetivos “en” o “cerca” del RPO/RTO.

Recovery Time Objetive: El tiempo objetivo de recuperación (RTO) es la duración del tiempo y un nivel de servicio dentro del cual se debe restaurar un proceso comercial después de un desastre (*entiéndase: cualquier situación anormal que afecte los procesos y funciones*) para evitar consecuencias inaceptables asociadas con una interrupción en la continuidad. En otras palabras, el RTO es la respuesta a la pregunta: "¿Cuánto tiempo me permito tardar en recuperarme después de la notificación de la interrupción del proceso comercial?"

Recovery Point Objetive: El punto objetivo de Recuperación (RPO) describe el intervalo de tiempo que podría pasar durante una interrupción antes de que la cantidad de

[29] Recovery Time Objetive
[30] Recovery Point Objetive

datos perdidos durante ese período exceda el umbral máximo permisible o "tolerancia" del Plan de Continuidad del Negocio.

Ejemplo: si la última copia buena disponible de los datos ante una disrupción es de 18 horas atrás, y el RPO para este negocio es de 20 horas, entonces aún estamos dentro de los parámetros del RPO del Plan de Continuidad del Negocio. En otras palabras, la respuesta a la pregunta es: "¿Hasta qué punto podría la recuperación del proceso empresarial proceder de manera tolerable dado el volumen de datos perdidos durante ese intervalo?"

Entonces, RPO designa la cantidad variable de datos que se perderán o tendrán que volver a introducirse durante, por ejemplo, el tiempo de inactividad de la red. RTO designa la cantidad de "tiempo real" que puede pasar antes de que la interrupción comience a impedir grave e inaceptablemente el flujo de las operaciones comerciales normales.

Siempre hay una brecha entre los reales tiempos aceptables y los objetivos introducidos por varios pasos manuales y automatizados para llevar la aplicación comercial. Estos datos reales solo pueden exponerse en los ensayos de desastre y de interrupción comercial.

El Ingeniero en Sistemas siempre está expuesto a pérdidas de datos, enlace, caída de servidores, interrupción de procesos y otras tantas. Ello conlleva a la importancia de ambos conceptos (RTO y RPO).

Objetivos más Generales del BIA:

Entre los objetivos más generales del BIA podemos encontrar:

- Identificar que todas las dependencias estén ingresadas en Archer, si no lo estuvieran identificar el owner CMDB (Configuration Management Data Base).
- Identificar que todas las aplicaciones estén ingresadas en Aris y si no estuvieran solicitar las actualizaciones.
- Analizar el impacto potencial en términos de una caída en los ingresos, incremento en los gastos operacionales y pérdida de confianza pública.
- Proveer documentación escrita de los posibles impactos, con el beneficio del contar con la documentación estandarizada y centralizada en Archer.

Pasos al Realizar un BIA:

Cada negocio de la empresa necesita analizar el impacto de una posible interrupción o pérdida de servicio haciendo un Análisis de Impacto de la Unidad de Negocio (BUIA). Este es el primer y más importante paso en el desarrollo de un programa de continuidad de negocios. Una salida de funcionamiento de un proceso o *outage* puede tener impactos cuantitativos o cualitativos dentro del negocio ya sean medidos en términos de consecuencias tangibles (pérdida de ingresos, disminución en la productividad de los empleados, etc.), o en contraposición aquellos que son medidos en términos de efectos intangibles (pérdida de confianza del cliente, diminución de la reputación de la empresa, impacto negativo en la moral de la empresa, etc.).

Al conducir un BIA se debería considerar los siguientes pasos:

- **Involucrar a las personas correctas.** Simplificará el proceso de hacer un BIA. Un ejemplo de cómo involucrar un especialista (subject matter expert) al proceso es: utilizar un contador senior para responder preguntas relacionadas al proceso contable o utilizar un owner o propietario de una aplicación informática para determinar si la aplicación/sistema es crítico para la BU.

- **Validación de los datos en Archer**. Recordar que los datos son almacenados en Archer, pero no mantenidos, por lo tanto, cualquier modificación debe ser realizada en la fuente.

- Dado que una de las diferencias principales respecto a métodos anteriores es la orientación a procesos, nuestro primer paso en esta etapa será **identificar los procesos** usados en la BU.

- Como los procesos deben estar alineados con los procesos de **Tartan** (a menos que la BU ya esté dentro de un rollout de **Tartan**), el próximo paso será **asociar los procesos de la BU con los major processes** definidos en **Tartan**.

- **Identificar las tecnologías** que soportan a los procesos establecidos en el paso anterior. Para cumplir este objetivo se utiliza Aris. Tal como se mencionó anteriormente, si la tecnología no se encuentra definida entonces debemos solicitar los cambios necesarios en el sistema fuente.

- **Definir las instalaciones** donde los procesos identificados se efectúan.

- **Evaluar los procesos**. Para ello se utilizan las herramientas más útiles y efectivas (entrevistas, enviar encuestas por mail, etc.) que nos permitan obtener información. Diseñar un **cuestionario a nuestra medida**, sin dejar de lado los aspectos cuantitativos y cualitativos, debe abordar preguntas tales como:
    - Existe un proceso alternativo registrado/documentado si las instalaciones o tecnologías no están disponibles? (Cadena de Suministros).
    - Qué tiempo de actividad de este proceso alternativo será considerada como tolerable? (Proceso de Ventas).
    - Si ocurre una interrupción de un proceso, cuál será la perdida estimada? (Transporte y Logística).
    - Cuál es el máximo tiempo de inactividad que el negocio puede soportar el proceso inactivo desde el punto de vista financiero y productivo?.
    - Cuál es el tiempo en que un cliente puede comenzar a perder confianza en nosotros por una caída de un proceso y su eventual inactividad lo que generaría un incumplimiento en nuestras obligaciones contractuales?.

Las respuestas a estas preguntas refleja la importancia de haber definido correctamente nuestro subject matter expert.

- **Elaborar ranking de procesos**: Una vez que las preguntas han sido respondidas, tenemos los recursos para **asignar un rango de criticalidad y los diferentes niveles de recuperación (tiers)** a los procesos.
    - Respuestas a las preguntas anteriores nos ayudarán a **dividir nuestros procesos en niveles en de criticalidad**. Los procesos con rango Critical, High y Medium son obligatorios, por política, de tener un BCP. Los procesos con rango LOW no son obligatorios en cuanto a BCP.
    - El RTO y RPO lo definimos en el análisis de respuestas a preguntas tales como: cuánto puede estar nuestra BU con un proceso inactivo sin ocasionar pérdidas significativas? Siendo estos dos indicadores (RTO y RPO) quienes también nos proporcionarán información para **clasificar los procesos en cuanto a capas (tiers) de recuperación**:

        Tier 1 – Vital

        Tier 2 – Corporate Critical

        Tier 3 – Mission Sensitive

Tier 4 – Business Tolerant

De un modo similar a las políticas para el BCP (en lo que respecta a criticalidades que lo hacen obligatorio), los DRP son obligatorios para las tecnologías (ej. Aplicaciones) con capa de recuperación (Tier) 1 a 3.

Los sistemas/aplicaciones con capa de recuperación (Tier) = 4 deberían tener un plan de DR pero no es obligatorio por política.

- **Crear el BIA en Archer**. Una vez que tenemos toda la información evaluada, el siguiente paso es crear un registro en Archer para nuestro BIA.
- **Solicitar la aprobación**. Luego que el BIA ha sido cargado en Archer, aguardamos su aprobación desde Mineapolis.

Hasta aquí, se ha enumerado los aspectos más importantes al considerar la realización de un BIA. Se le ha dado relevancia, como base del conjunto de planes que integran el Reciliency Management. Los demás planes descriptos a continuación, serán abordados de una forma más superficial puesto que el autor, al igual quienes integraban el equipo de **TGRC**, entiende: todo el desarrollo posterior está supeditado a una correcta definición y elaboración del BIA.

8.4 Plan de Continuidad de Negocio o Business Continuity Plan (BCP)

Mensaje Principal de Necesitar un BCP:

El fundamento o justificación principal de un Programa de Continuidad de Negocio es asegurar la continuidad de ejecución de los procesos, al menos esenciales, durante un evento que cause una interrupción en instalaciones, tecnología, empleados o cualquier otra área dentro de la organización. Lo que podría suponer la siguiente idea organizacional: seguimos produciendo, aún, durante una contingencia que cause disrupciones.

Método Previo:

- Plan de Continuidad de Negocio era ad hoc, donde documentos y planes se pensaban o desarrollaban de forma particular sitio a sitio.
- BCP no estaba basado en una definición de procesos.
- Los diferentes planes no eran almacenados o gestionados centralmente.
- No había reportes estandarizados.

Método Actual:

- Cada unidad de la empresa o función, debe completar su BCP anualmente.
- El BCP evalúa enfocándose en los principales procesos de negocio, como lo exige el **Tartan Project**.
- BCP no focaliza eventos puntuales como fuego e inundación, más bien lo hace sobre un número de factores que incluyen:
    - Empleados
    - Instalaciones
    - Tecnología
    - Cadena de proveedores
- Herramienta empresarial disponible, Archer:
    - Consistente
    - Aproximación formal
    - Centralizada
    - Reportes estandarizados
- Revisión de procesos exigida:
    - Requerida dos veces por año para cada BU/Función
- Prueba de procesos exigida:
    - Anualmente requiere pruebas para cada proceso de negocio que haya sido ranqueado con el índice de crítico, alto o medio.
    - Revisión anual de los resultados de las pruebas para cada BU/Función.

Se puede apreciar en BCP, a diferencia de BIA, comienza a ganar preponderancia las pruebas frente a otros factores. A los diferentes tests se les asigna una propiedad transitiva en la empresa, es decir, si la prueba es incorrecta o no satisface las metas entonces la definición del BIA ha sido deficiente.

Objetivos y Principales Características del BPC:

El Business Continuity Plan, es un esfuerzo de planificación y preparación para toda la organización destinado a garantizar que la empresa mantenga sus operaciones esenciales durante y después de incidentes disruptivos. A fines de 2016, la empresa contaba con 160.000 empleados y tenía presencia en más de 70 países, donde cada BU necesitaba elaborar evaluaciones de continuidad del negocio iniciadas en la herramienta de planificación Archer.

Con esta planificación, la empresa cuenta con un proceso que se utiliza para desarrollar un plan práctico de cómo se podría recuperar o restaurar parcialmente

actividades comerciales críticas dentro de un marco de tiempo predeterminado después de una crisis o desastre. El plan resultante se llama Plan de Continuidad del Negocio (BCP).

Como parte de todo el proceso de desarrollo, el Plan de Continuidad del Negocio también debe poseer ensayos, mantenimiento y revisión de los componentes donde se tomen medidas para garantizar que los planes continúen satisfaciendo las necesidades de la empresa a lo largo del tiempo.

Dependiendo del tamaño y la naturaleza de la BU/Función, se puede optar por tener Planes de Administración de Riesgos, Análisis de Impacto Comercial, Respuesta y Recuperación por separado, o para una pequeña unidad, un solo plan que incorpore todos los elementos anteriores puede ser suficiente. En el caso de la empresa en cuestión, es indudable que se necesita una modularidad de planes que en su conjunto conforman el Reciliency Managent Plant.

Pasos al Realizar un BCP:

Si la BU/Función no cuenta con un plan BC implementado, como el caso de Beef Argentina que fue adquirida a Finexcor, se comienza por evaluar sus procesos comerciales, determinar qué áreas son vulnerables y las posibles pérdidas si esos procesos disminuyen durante un día, unos días o una semana. Esto es esencialmente un BIA, definido anteriormente.

A continuación, se desarrolla un plan. Esto implica los siguientes pasos generales**:**

- **Identificar ambiente o alcance del plan**. Punto de partida para indicar sobre la BU/Función que será desarrollado y desplegado el plan. Generalmente el ámbito, según especificaciones de **TGRC**, será todo el personal localizado y todos los procesos que se ejecuten en la BU/Función. Significa, el plan inicia considerando todo lo mencionado anteriormente.
- **Identificar participantes**. Escoger correctamente a las personas que se involucrarán en la construcción del BCP de manera de hacer su creación, un proceso suavizado.
    - Identificar a los participantes quienes asistirán en la creación del BCP.
    - El BCP es conducido por el BIA, involucrando a miembros del equipo BIA que sean más beneficiosos.
    - Contar con los SME (Subject Matter Expert) relacionado a los procesos de negocios y la revisión de resultados BIA y desarrollo de alternativas

de trabajo para soluciones de procesos críticos, altos o medios (critical, high o médium).
    - Delinear el rol de IT, pero en ningún caso ese rol debe ser el rol SME para los procesos de negocio.
- **Brindar acceso**. Antes de comenzar con la etapa de análisis de los procesos y relaciones, se debe asegurar que el equipo de BCP tendrá acceso al material necesario almacenado y centralizado en Archer.
    - TRCMs son responsables de aprobar los requerimientos de adicionar Coordinadores de Contingencias o Resiliencias en la herramienta Archer a través de los permisos administrativos de la herramienta.
    - Coordinadores de Contingencias o Resiliencias son responsables de aprobar los requerimientos de adicionar "especialistas", por ejemplo, desde Recuperación de Desastre (DR), Continuidad de Negocios (BC) hasta la herramienta Archer a través de los permisos administrativos de la propia aplicación**.**
- **Validación de los datos**. Es recomendable, antes de iniciar un BCP, efectuar una revisión exhaustiva de los resultados del BIA.
    - Comprender cuales procesos son realmente importantes, ellos ayudarán en la priorización.
    - Los datos específicos de la empresa no son mantenidos en Archer, así que deben ser corregidos en el registro de la fuente.
    - Obtener una lista de las facilidades o locaciones que el analista validará y desplegará para ser registradas en Archer. En el caso del autor, se ha mencionado el alcance era Planta Bernal y Planta Nelson, es decir, dos facilidades cuyos datos debían ser validados.
- **Validación de las facilidades**. Al validar los datos anteriormente mencionados, también se estará validando las facilidades, creando su respectivo registro en Archer.
- **Localizar y especificar las relaciones entre áreas y funciones en la BU como también los procesos indispensables**. Es común, en empresas de producción, un proceso no poder iniciar si aún no se completó o no generó la información suficiente algún otro proceso. Todas estas relaciones deben ser encontradas, la razón de la mención es que algunas son obvias, otras no resultan tan apreciables a simple observación del analista. En el caso particular del trabajo en la empresa, se encontraron más de 20 relaciones "ocultas" entre procesos, áreas o funciones; lo que habría constituido un grave error. También se determinarán aquellos procesos indispensables que requieren continuar operando aun en tiempo de disrupciones.

- **Especificar la copia de seguridad, o backup de los datos, y el plan de recuperación**. El BCP debe especificar de forma clara los procedimientos de backup y recuperación de datos.
    - La frecuencia con que se realizan las copias de seguridad como así también el responsable.
    - Dónde se almacenan los datos y como se replican geográficamente para que ningún desastre local pueda ocasionar una perdida permanente.
    - El procedimiento para iniciar la recuperación de los datos.

  Estas cuestiones deben abordarse tanto para los registros en papel, como para los electrónicos. En el caso de la planta responsabilidad del autor, los analistas determinaron el backup de los datos electrónicos del servidor se hagan a la medianoche de cada día. Lo que implica, una contingencia o evento disruptivo iniciado al mediodía significa una pérdida de datos de las últimas 12hs de vida de la BU. Cómo es posible aceptar la situación? Sí, performance. El flujo de datos en la red, la información productiva, de carga, gubernamental, actualizaciones de topología en los routers, protocolos de seguridad, solicitud/respuesta de todos los PLC (Controladores Lógicos Programables) Siemens dispuestos en planta y otro tipo de datos intercambiados entre dispositivos electrónicos haría insostenible la realización de backups en horarios de producción completa. El período de tiempo entre copias de seguridad es el precio pagado para lograr buen desempeño o performance… razonable.

- **Determinar el tiempo de inactividad aceptable para cada función crítica**. Los SME aseguran una respuesta correcta a este interrogante.
- **Crear un plan para mantener las operaciones de los procesos obtenidos en los puntos anteriores**. Todas las BU/Funciones se requiere tengan desarrollado al menos un BCP, el cual cubre todos sus procesos de negocios con índice crítico, alto y medio. Esto se alinea con las políticas del Resiliency Management Plan, la continuidad de negocio asociada con el BIA y la descripción en detalle de las estrategias alternativas de procedimientos.
- **Comunicación.** La comunicación requerida para que todas las personas involucradas puedan conocer su rol en la continuidad de los procesos establecido. ¿Cómo se notificará al equipo de BCP de una emergencia si, por ejemplo, se interrumpe el procesamiento de datos? ¿Quién está autorizado a hablar en nombre de la empresa a los clientes, proveedores y socios externos?

El plan debe incluir una lista de personas y equipos que serán contactadas cuando se declare una emergencia.

- **Prueba.** Un BCP que se ve bien en papel puede ser totalmente inviable en la práctica. Debe ser probado de manera realista antes de que se ponga en funcionamiento, y los empleados clave entrenados en su uso. Luego debe actualizarse regularmente. Con las condiciones cambiantes, la tecnología, las estructuras organizativas y el personal, el plan puede quedar obsoleto e inutilizable rápidamente. Los procedimientos para la capacitación, para probar y actualizar el plan deben incluirse en el BCP mismo. Como señala el Departamento de Seguridad Nacional de EEUU, "un plan de continuidad comercial para continuar con los negocios es esencial". Lograr el alcance del plan de continuidad comercial es crucial para la capacidad de supervivencia de la empresa en caso de que ocurra un desastre. Desarrollar y mantener un buen BCP puede parecer una tarea desalentadora. Pero si el ingeniero responsable está listo y capacitado para enfrentar el desafío, se puede proteger a la empresa del desastre.

Estructura de un BCP:

En el siguiente gráfico se puede observar la estructura de un Business Continuity Plan, implementado por la empresa.

El propósito del “árbol de llamadas” o Calling Tree para cada proceso, es contar con un método eficiente que asegure a los miembros del equipo serán contactados e informados durante una crisis, desastre o cualquier otra disrupción que ocurra en una locación. Es una “hoja de cálculo” o planilla que detalla BU/Función, líder, teléfonos, tipo te acceso remoto, confirmación de contacto, etcétera. Usada para confirmar contactos de los empleados que brindarán ayuda y establecerán los procesos de recuperación necesarios.

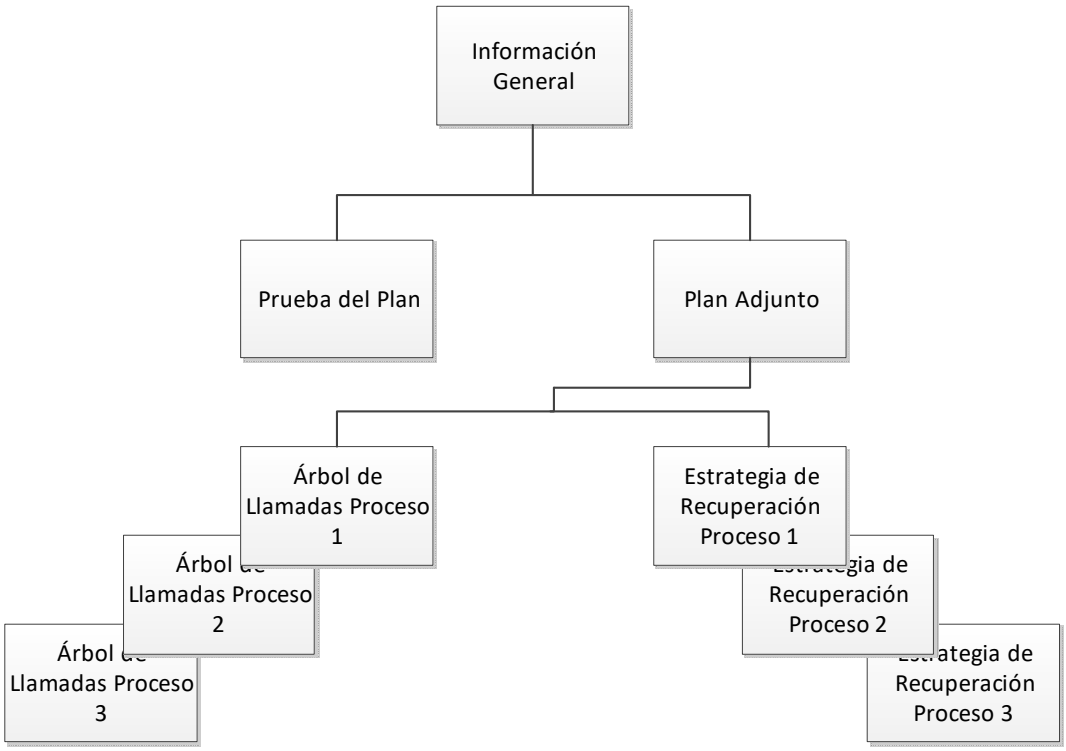


Figura 19. Estructura del BCP.

8.5 Plan de Recuperación de Desastres (DRP)

Mensaje Principal de Necesitar un DR:

Las empresas utilizan la tecnología de la información para procesar datos de manera rápida y efectiva. Los empleados utilizan el sistema de correo electrónico y el sistema telefónico de Voz sobre Protocolo de Internet (VOIP) para comunicarse. El intercambio electrónico de datos (EDI) se utiliza para transmitir datos, incluidos pedidos y pagos de una compañía a otra. Los servidores procesan información y almacenan grandes cantidades de datos. Las computadoras de escritorio, las computadoras portátiles y los dispositivos inalámbricos son utilizados por los empleados para crear, procesar, administrar y comunicar información. ¿Qué se hace cuando la tecnología de información deja de funcionar?.

El Plan de Recuperación de Desastres o Disaster Recovery Plan engloba aquellos planes que aseguran el restablecimiento de las aplicaciones, tecnologías y sistemas después de un evento disruptivo. El BIA ha identificado las aplicaciones, sistemas y tecnologías que necesitaran ser recuperadas a través del correspondiente plan.

Método Previo:

- Plan de Recuperación de Desastres era realizado ad hoc y variaba ampliamente de una BU a otra.
- RTOs y RPOs no eran definido claramente.
- No se alineaba con las capacidades de recuperación.
- Los planes no eran almacenados o gestionados de forma centralizada.
- Reportes estandarizados.

Método Actual:

- DRPs son basados en los RTOs y RPOs identificados como resultado del proceso BIA.
- DRPs hacen foco en la recuperación de sistemas técnicos (uso de tecnología); NO procesos de negocios, gestión de crisis o comunicación.
- Un DRP puede recuperar uno o más sistemas, aplicaciones o tecnologías.
- Uso de herramienta empresarial, Archer:
    - Consistente
    - Aproximación formal
    - Centralizada
    - Reportes no estandarizados
- Proceso de revisión:
    - Requiere de dos revisiones anuales por BU/Función.
- Proceso de prueba:
    - Tiers 1, 2 y 3 serán testeados anualmente.
    - Los resultados de las pruebas serán revisados cuidadosamente por la BU/Función.

Objetivos y Principales Características del DRP:

El Disaster Recovery Plan es un conjunto de planes técnicos que contienen información detallada de CÓMO restaurar los sistemas afectados en un evento disruptivo.

El objetivo de los DRPs es asegurar que las aplicaciones, sistemas o tecnología serán restaurados dentro de los designados: Tiempo Objetivo de Recuperación y Punto Objetivo de Recuperación (RTO y RPO respectivamente).

Se debe desarrollar un plan de recuperación ante desastres de tecnología de la información (IT DRP) junto con el plan de continuidad del negocio. Las prioridades y los objetivos del tiempo de recuperación para la tecnología de la información deberían

desarrollarse durante el análisis del impacto comercial. Deben desarrollarse estrategias de recuperación de tecnología para restaurar el hardware, las aplicaciones y los datos a tiempo para satisfacer las necesidades de la recuperación comercial.

Las empresas grandes y pequeñas crean y administran grandes volúmenes de información o datos electrónicos. Gran parte de esa información es importante. Algunos datos son vitales para la supervivencia y la operación continua del negocio. El impacto de la pérdida o corrupción de datos por fallas de hardware, errores humanos, piratería informática o malware puede ser significativo. Un plan de copia de seguridad de datos y restauración de información electrónica es esencial.

A continuación, se enumeran algunos de los aspectos delineados dentro de la empresa para un DRP aconsejado.

Estrategias de recuperación de IT. Se debe desarrollar estrategias de recuperación para sistemas, aplicaciones y datos de tecnología de la información. Esto incluye redes, servidores, computadoras de escritorio, computadoras portátiles, dispositivos inalámbricos, datos y conectividad. Las prioridades para la recuperación de IT deben ser coherentes con las prioridades para la recuperación de las funciones y los procesos comerciales que se desarrollaron durante el análisis de impacto de negocio. El tiempo de recuperación para un recurso de IT debe coincidir con el objetivo del tiempo de recuperación para la función de negocio o el proceso que depende del recurso de IT.

Algunas aplicaciones comerciales o de negocio no pueden tolerar ningún tiempo de inactividad. Utilizan centros de datos duales capaces de manejar todas las necesidades de procesamiento de datos que se ejecutan en paralelo con los datos duplicados o sincronizados entre los dos centros. Esta es una solución muy costosa que solo las compañías más grandes pueden pagar. Algunos datos dentro de la empresa de referencias utilizaban el método mencionado, aun siendo costoso. Duplicación y sincronización eran de un costo menos elevado que la perdida de datos o tiempo de recuperación.

Estrategias de recuperación interna. Muchas empresas tienen acceso a más de una instalación, en el caso del autor: Bernal y Nelson. El hardware en una instalación alternativa se puede configurar para ejecutar aplicaciones de hardware y software similares cuando sea necesario. Suponiendo que los datos se respalden fuera del sitio o que los datos se reflejen entre los dos sitios, los datos se pueden restaurar en el sitio alternativo y el procesamiento puede continuar. Dado que la empresa poseía solo una licencia de Unix, el servidor se localizaba en Bernal, pero una copia de seguridad de

datos estaba en Nelson, junto a un backup del servidor; por lo que una caída en Bernal permitía operar con Nelson como servidor principal.

Copias de seguridad. La empresa generaba grandes cantidades de datos y los archivos de datos cambian a lo largo de la jornada laboral. Los datos pueden perderse, corromperse, comprometerse o ser robados debido a fallas de hardware, errores humanos, piratería y malware. La pérdida o corrupción de datos podría ocasionar una interrupción comercial significativa. La copia de seguridad y recuperación de datos era una parte integral del plan de continuidad del negocio y del plan de recuperación de desastres de la tecnología de la información. El desarrollo de una estrategia de copia de seguridad de datos comienza con la identificación de los datos a respaldar, seleccionando e implementando procedimientos de respaldo de hardware y software, programando y realizando respaldos y validando periódicamente que los datos se hayan respaldado con precisión.

Desarrollar un plan de recuperación de desastres de IT. La empresa desarrolló un plan de recuperación ante desastres de IT. Comienza compilando un inventario de hardware (por ejemplo, servidores, computadoras de escritorio, computadoras portátiles y dispositivos inalámbricos), aplicaciones de software y datos. El plan debe incluir una estrategia para garantizar la copia de seguridad de toda la información crítica. Se identificaban las aplicaciones de software críticas y los datos y el hardware requerido para ejecutarlos. Usar software estandarizado ayuda a replicar y volver a crear imágenes en el nuevo hardware. Se contaba con “imágenes TCO” del software necesario para operar una computadora en cualquier parte del mundo, lo que agilizaba el proceso de recuperación.

Han sido solo algunas de las características del DRP implementado por la organización.

8.6 Planificación de Gestión de la Crisis (CMP)

Mensaje Principal de Necesitar un CMP:

En nuestra era de excesivo dinamismo, impulsado por la tecnología, las crisis digitales pueden afectar en cualquier momento. Y cuando lo hacen, se propagan rápidamente, viajando a través de las redes sociales y los sitios de noticias en línea más rápidamente que nunca. Cuando algo va mal en la organización, millones de personas pueden enterarse en cuestión de minutos. No es de extrañar que cada año que pasa se centre más en el manejo digital de crisis.

CMP es la acción de comandar y controlar las acciones durante una crisis o evento disruptivo, en el cual la organización se predispone de una manera más favorable a enfrentar estos eventos.

El comando y control, en la empresa, se relacionaba a las personas o partes interesadas quienes eran designados desde Mineapolis en acuerdo con la gerencia de la BU y con asesoramiento del RCC (en el caso de estudio el rol lo desempeñaba el autor del presente trabajo), por lo que no se brindaran mayores detalles.

8.7 Plan de Pruebas o Tests

No se abordará en mayores detalles en el presente trabajo. El autor considera ha dado suficientes datos en cada desarrollo anterior, sobre exigencias de desarrollo.

Mensaje Principal de Necesitar un Plan de Pruebas:

Con un conocimiento profundo de las interacciones necesarias entre IT y la empresa, se ha ayudado a alinear las áreas para que se pueda probar y validar los planes de resiliencia de su BU/Función.

La organización central exigía pruebas al menos dos veces en el año con revisión de los resultados. Toda la información relevante debía cargarse en Archer, de haber una disconformidad, la misma era informada para proceder a efectuar los cambios necesarios.

9 CONCLUSIONES

9.1 Consideraciones Generales del Proyecto TGRC, su Relación con la Organización

La empresa ha ganado conciencia sobre la implicancia de los riesgos en especial aquellos tecnológicos e informáticos y, sobre todo, aprendió de la experiencia que generalmente debe coexistir con los mismos, lo que implica hacerlo de manera controlada.

Nuevas amenazas se detectan día a día sobre los servicios de IT y se ha exigido desde Mineapolis un análisis de riesgo y un plan de mitigación, aún con estas consideraciones, la empresa entiende que siempre quedará un riesgo remanente y latente en sus procesos de misión crítica. Lo que conduce a la definición de continuidad del negocio.

El método utilizado, centralizado y global, hace que sea relativamente sencillo desplegarlo en un marco mundial de aproximadamente 77 países, puesto que todos los integrantes del equipo -situados en diferentes lugares- “hablan el mismo idioma”. Lo que implica mejor comunicación, trabajo en equipo, coordinación y colaboración entre otras tantas virtudes.

Una vez establecida una línea base de objetivos y metas, a corto y largo plazo, se puede determinar qué constituye el éxito o fracaso del proyecto. Aquí el protagónico lo asumen las métricas. La recolección de datos y construcción de mediciones en forma

mensual, permite una aproximación fundamental del modo en que el plan se está desplegando a nivel mundial. Es por demás elocuente que, al ser un proyecto de alcance mundial, la organización central debe tener la herramienta necesaria y suficiente de control para la monitorización de evolución del proyecto. Implementando las medidas de corrección necesarias ante situaciones de desvíos en desempeño de la performance esperada.

La centralización de las políticas y su almacenamiento, permite no solo un mejor control en la aprobación para los supervisores en US, sino también un mejor acceso como repositorio de guía y consulta permanente por la propia Unidad de Negocio que lo ha definido y por aquellas emergentes que muchas veces solo cuentan con una vaga idea, no desarrollada, sobre procesos.

Coordinación de los roles es una de las esencias del proyecto. Cómo coordinar unidades de negocios en más de76 países si no se definen roles o, aun definiendo roles, no se cuenta con la herramienta necesaria?. El “arte de coordinar”, la empresa perseguía ese concepto a sabiendas de que era la columna vertebral del éxito. Las técnicas adecuadas implementadas y enumeradas en el presente trabajo, ayuda a los coordinadores a satisfacer las necesidades, al garantizar que el proyecto permanece a tiempo, dentro del presupuesto y bajo control. Archer y Altiris constituían la herramienta de software centralizada y desplegable a medida de las ambiciosas necesidades del Proyecto **TGRC**.

En cuanto a la definición e identificación de procesos, contábamos con una completa gestión de procesos de negocios reunidas en un conjunto de prácticas centradas en impulsar el valor de la compañía a través de una cultura de mejora de los procesos. Tarea que podía ser tan simple como definir procesos poco claros, localizar áreas de mejora y efectuar cambios, o tan compleja como una actividad de reingeniería de procesos productivos y comerciales cuasi completos. La identificación y priorización que hacíamos de los procesos encontrados, era la base de la siguiente etapa (Resiliency Management) o la comprensión de un nuevo enfoque ya no orientado a funciones sino a procesos. Cualquiera sea la perspectiva desde donde se lo aborde, sin dudas encontrábamos innumerables beneficios.

El hecho de conocer los marcos de referencias para el análisis de riesgo no asegura que el proceso se lleve a cabo en forma exitosa. Por esto, se requería adicionalmente de una metodología que, en forma eficaz y eficiente, aplique los marcos de referencias exitosamente en la labor del análisis de riesgos de IT. Lo anterior conlleva a que se identifiquen y prioricen exhaustivamente los diferentes riesgos para definir planes de

acción y de protección, acordes con cada uno. La labor en general no fue una tarea fácil, ya que involucraba un estudio detallado de todas las áreas de la organización y un análisis crítico que garantice la adecuada identificación y priorización de los riesgos y vulnerabilidades. Se hizo necesario, entonces, contar con metodologías que faciliten el logro de estos objetivos de altos volúmenes de información.

Como consecuencia de lo expuesto, organizativamente, se contaba con todo lo necesario para desplegar un proyecto de esas características y perseguir metas extremadamente ambiciosas que no solo logren mayor eficiencia corporativa sino permita certificar los más altos estándares internacionales.

9.2 Consideraciones Generales del Proyecto TGRC, las Percepciones del Autor

A partir de la experiencia vivida y relatada -en profundidad- en la presente memoria técnica, el autor puede concluir que las metodologías ágiles de gestión de proyectos utilizadas corporativamente, son de gran valor a la hora de encarar proyectos de corta duración o aquellos de larga duración, es decir, son tan valiosas tanto para lograr conformidad en urgentes aspectos de seguridad en servidores como para alinear mundialmente la corporación a un plan de contingencias, solo por citar dos ejemplos válidos. Estos métodos eran la única forma posible de adaptarse al dinamismo que involucra al ámbito de la organización, no solo para ella sino también para clientes y proveedores.

Como este tipo de métodos ágiles de gestión de proyectos tienen su origen en los proyectos informáticos, el autor no solo poseía experiencia frente a líderes que pertenecían a otras áreas, sino también logró un entrenamiento y experiencia significativamente importante que le permitió posicionarse adecuadamente a las necesidades laborales de empresas que intentan implementar una adecuada gestión de riesgos.

El Gobierno y Control de los Riesgos Tecnológicos o **TGRC**, ha ganado importancia y difusión en estos días por lo ocurrido en FACEBOOK. Suponiendo que en verdad no se suministraron datos voluntariamente, se demuestra la importancia de poseer en toda empresa un plan de estas características que aborde la problemática y lo gestione adecuadamente. El autor considera que la mejor forma es hacerlo como la empresa en cuestión donde un conjunto de módulos, planes, herramientas y equipos constituyen el plan general. Todos y cada uno de los puntos desplegados en el trabajo hacen posible el Control y Gobierno de los Riesgos. Una vez que una potencial amenaza se

transforma en ataque real, la imagen de la empresa frente a la competencia sufrirá un daño que en muchas veces es irreparable en confianza de clientes, proveedores o público en general.

El autor logró posicionar, antes del traspaso hacia Friar, a Cargill Beef Argentina como la mejor Unidad de Negocio de la corporación a nivel mundial en lo que respecta a seguridad informática en conformidad y alineación a los objetivos del **Proyecto Tartan**.

9.3 Consideraciones Generales del Proyecto TGRC, Principales Desafíos

Al tiempo de enumerar desafíos, el autor principalmente extrae en relevancia, dos aspectos:

Incorporar la idea de Beneficios Intangibles

Aunque parezca una verdad de Perogrullo, la mayoría de los gerentes de producción no comprendían que ciertos beneficios son intangibles al corto plazo, pero son muy redituables a futuro. No entendían la necesidad de reunirse y destinar treinta minutos semanales o una hora a identificación y revisión de procesos, estimaban que producir solo daría ganancias sustanciales. Por este motivo, el apoyo brindado al autor desde Mineapolis fue inmenso, desde sanciones a personas con puestos importantes a email que inducían a colaborar sí o sí.

De este modo, el 90% del BIA en cuanto a objetivos propuestos, fue alcanzado satisfactoriamente, el 99.8% de conformidad en parches de servidores y computadoras, el 40% en reducción de inconformidades en caminatas de control o walkthrough, el 60% de disminución en irregularidades de cuentas y accesos, solo por citar algunos logros.

Solo fue posible con la consideración que, aun, un gerente era un “cliente” no técnico que se debía convencer sobre los beneficios del proyecto.

Incorporar la idea de “procedimiento de trabajo” y “trabajo en equipo”

La pregunta del lector sería: no hubo errores?. La respuesta es: por supuesto que los hubo.

Procedimiento es la palabra o concepto fundamental en toda organización proveniente de US. Los gerentes principales esperan actividades y acciones guiadas por

procedimientos. Ante una inconformidad de alguna meta, no esperaban excusas, sino percibir que habíamos encontrado el procedimiento para no caer en el mismo error en la siguiente métrica.

Si bien la idea fundamental es fácilmente interpretada y comprendida por alguien relacionado a sistemas, este concepto no resulta tan entendible por el sector productivo que involucra gerentes de producción y supervisores. Imagine un analista preguntando: cómo se hace?, Por qué se hace así?. Suena a indagatoria en el mejor de los casos. En el peor, suenan respuestas tales como: porque siempre se hizo así!. Es común en organizaciones de origen familiar (como Finexcor) que ciertos procedimientos tienen origen en causas que dejaron de ser válidas.

El ***trabajo en equipo*** constituyó otro escollo en el despliegue del plan. Es más difícil de lo que parece lograr una participación activa de todos los involucrados, ello implica dejar de lado egos, cambio radical de actitud y asumir errores o aceptar modificaciones en sus actividades.

La habilidad del profesional es inducir a un cambio de actitud en toda la organización, trabajar en equipo no siempre es fácil o se logra plenamente. Regirse por procedimientos y trabajar en equipo significaba 90% del éxito en la corporación.

ANEXO I: ROLES

➢ RCC/TRCC/SRCC

La siguiente es una lista de las actividades desplegadas por el autor y exigidas desde Mineapolis, con su correspondiente periodicidad.

Semanal

- Revisar el reporte de software “desconocido”.
- Validar cualquier cambio del software y los procesos requerido tendiente a legitimarlos.
- Crear la no conformidad en una hoja de cálculo y cargarla dentro de una herramienta de “auto email”.
- Determinar si se requiere alguna traducción para el no cumplimiento. Traducir y reenviar al empleado/gerente.
- Gestionar y administrar los procesos y procedimientos para los softwares no reconocidos dentro de la BU y coordinar con la Plataforma/SAM.

Mensual

- Distribuir las comunicaciones y conocimientos de TGRC al sitio RCC.
- Asegurar la traducción al lenguaje nativo de lo anterior
- Validar que el mensaje ha sido entregado en la BU, RCC y continuar con cualquier deficiencia descubierta.
- Gestionar y administrar la conformidad local de remoción o validación del software instalado.
- Revisar reporte eliminación vs compra y encontrar entradas negativas para la BU
- Encontrar usuario/s en nueva lista de instalación.
- Validar cualquier cambio en los procesos o software requerido para el registro de la legitimidad del software.
- Revisar punto por punto todos los reportes y respuestas.

Trimestralmente

- Monitorear por completo la realización (o realizarlos) de los walkthrough.
- Asegurar cada sitio RCC ha entregado el material de conocimientos generados a los empleados involucrados.

Anualmente

- Revisar la guía de entrenamiento del RCC.
- Revisar la guía del sitio de contacto para limpieza de disco (disk wipe).
- Completar el BIA para cada aplicación de la BU.
- Actualizar el repositorio del BIA y el seguimiento de TGRC para las aplicaciones que son completadas.
- Desarrollar y mantener el DR Plan.
- Probar el DR Plan.
- Definir los procesos para acceso lógico de la información en ambiente - servidores, base de datos, aplicación, etc.- para cada responsabilidad de la BU.
- Llenar o diseñar la evaluación SecurCompass.
- Completar el entrenamiento COMPLETO en evaluación de SecurCompass.

Cuando sea necesario

- Entregar el entrenamiento a un nuevo RCC (si fuera aplicable).
- Servir como punto de contacto para las cuestiones y procedimientos de control y coordinación del riesgo.
- Trabajar con el RCC de la BU para asegurar los controles de limpieza de disco como sea necesario (disk wipe).
- Asegurar que el proceso disk wipe fue desempeñado correctamente.
- Asistir a los equipos locales en la adquisición de un nuevo software.
- Asegurar que todo el HW dispuesto en la organización es regulado y tiene aprobado el servicio.
- Supervisar el reemplazo de HW global de la corporación en cuanto a procesos y procedimientos exigidos por TGRC SAM.
- Revisar documentación.
- Identificar áreas de seguridad en proyectos.
- Documentar requerimientos de seguridad en proyectos (pre-diseño).
- Incluir el estado de riesgo y seguridad en la revisión de estado y etapas del proyecto.
- Participar en todas las reuniones como consejero en cuestiones de riesgo y control.
- Asistir con la documentación de administración y gestión de excepciones de varianzas.

➢ TECHNOLOGY RISK AND CONTROL COORDINATOR

La siguiente es una lista de las actividades desplegadas por el autor y exigidas desde Mineapolis, con su correspondiente periodicidad.

Mensual

- Revisar la conformidad de los reportes y asegurar que las acciones tomadas conducen a el cumplimiento de las políticas/objetivos de la BU/Función.
- Auditar dispositivos en la BU/Función (antivirus y parches).
- Asegurar que el proceso de limpieza de discos es desplegado correctamente en la BU/Función.
- Asegurar que la el procedimiento de limpieza de discos está siendo ejecutado correctamente por el RCC del sitio (cuando se colaboraba con otras BU).
- Ejecutar la auditoría efectuada anteriormente en parches y antivirus.
- Gestionar la conformidad local de validar o remover el software instalado.
- Revisar la instalación vs reportes de compras y encontrar entradas negativas para la BU.
- Encontrar usuario/s en nueva lista de instalación
- Validar el software y proceso para cualquier cambio requerido en cuanto a su legitimidad.
- Crear hoja de cálculo de no legitimidad y cargar en una herramienta de auto-email.
- Determinar si son requeridas traducciones para requerimiento de software y el mismo email, enviar al empleado/gerente.
- Gestionar los procesos SAM dentro de la BU y coordinar con la Plataforma/Función.

Anualmente

- Coordinar la revisión, actualización y prueba del Disaster Recovery Plan usando como entrada el detalle de la evaluación Business Impact de los procesos para la BU/Función dentro de la unidad anual de referencia.
- Coordinar la actualización anual de Guía de Soluciones/SecurCompass.
- Evaluar los accesos lógicos en aplicaciones.
- Monitorear y comunicar el progreso de remediaciones de brechas encontradas en las conformidades.
- Completar los BIAs para cada aplicación que lo requiera dentro de la BU.

- Desarrollar y mantener el Disaster Recovery Plan.
- Probar o testear el Disaster Recovery Plan.

Cuando sea necesario

- Coordinar la revisión regular y los procesos de aprobación de los accesos lógicos para las aplicaciones dentro de la carpeta o portfolio de la BU.
- Coordinar y asegurar que todas las brechas en el cumplimiento de las políticas tienen varianzas en la BU, compensando con los trabajos de control que se han definido para la excepción. Esto incluye TGRC y Varianzas.
- Coordinar la elaboración y terminación de toda la evaluación de los índices de riesgos que son requeridos por TGRC (Aplicación, Proveedor de Servicios de Aplicación, etc.)
- Coordinar y asegurar se toman las acciones tendientes a reunir o alinear a la definición KRA para el scorecad de TGRC.
- Implementar las acciones de riesgo en dirección de los riesgos tecnológicos.
- Asistir al equipo local en la adquisición de nuevo software.
- Revisar los requerimientos para nuevo software y aprobar cuando se necesite.
- Completar en Archer la evaluación requerida por TGRC en evaluación de aplicaciones.
- Revisar los requerimientos para la aprobación e instalación extra de software cuando sea necesario.
- Localizar las facturas y licencias para productos cuando sea requerido.
- Asegurar que el HW es colocado con una aprobación servicio dentro de lo solicitado por la empresa.
- Gestionar los procesos de remplazo global del HW y coordinar dentro de los estándares solicitados por TGRC SAM.
- Solucionar las brechas de conformidad encontradas en los accesos lógicos.
- Definir los procesos para los accesos lógicos en el sitio (servidor, base de datos, aplicaciones, etc.).
- Generar la lista de control de accesos para revisión del responsable representativo de la BU.
- Enviar el requerimiento para eliminar/cambiar registros en la lista de control de accesos.
- Monitorear la completa revisión de los procesos de accesos lógico.
- Revisar SOW (Statement Of Work, Estado del Trabajo) de proyectos y documentación requerida.
- Documentar requerimientos de seguridad (pre-diseño) dentro de los proyectos.

- Incluir riesgos de seguridad en estado de proyectos y revisión de etapas.
- Validar los requerimientos de remediación y dejar de medir la brecha (o inconformidad) del Plan para procedimientos abiertos.
- Discutir la variabilidad y planificación del presupuesto para esfuerzo de remediación.
- Coordinar y documentar los pasos provisorios de remediación para la BU en acuerdo a lo requerido y documentado por TGRC.
- Asistir en la creación de los planes de acción direccionados a correcciones a largo plazo o a correcciones permanentes a través de la Plataforma/Servicio Compartido.
- Asegurar que los planes de acción de auditoría son implementados.
- Participar en Consejo Asesor del Cambio (Change Advisory Board, CAB) y reuniones para control y riesgos requeridas.
- Crear y documentar varianzas.
- Revisar y renovar varianzas.
- Revisar y retirar varianzas.
- Eliminar borrador y rechazar varianzas.
- Asegurar a terceros (Third Parties) completar los Acuerdos de Acceso a la Red (Network Access Agreements, NAAs).

➢ SITE RISK AND CONTROL COORDINATOR

La siguiente es una lista de las actividades desplegadas por el autor y exigidas desde Mineapolis, con su correspondiente periodicidad.

Mensual

- Traducción para lenguajes diferentes al inglés.
- Comunicar los conocimientos, a través de email, a los empleados.
- Coordinar o entregar “cara a cara” el material de entrenamiento.
- Desplegar los carteles de conciencia.

Trimestral

- Completar las caminatas de control o walkthrough y log de excepciones.

Anualmente

- Revisar la guía de entrenamiento RCC.
- Revisar la guía del sitio de contacto para la limpieza de disco (disk wipe).
- Acceso lógico.

Cuando sea necesario

- Asegurar los acuerdos de accesos a la red (NAA) han sido completados.
- Asegurar que el disk wipe es hecho en el sitio.
- Hacer disk wipe local.
- Hacer disk wipe remoto.
- Servir para punto de contacto para riesgo y control en consultas y procedimientos.
- Wipe HD.
- Asegurar el HW es dispuesto dentro del servicio aprobado por la empresa.
- Remediar las brechas en acceso lógico dentro de las aplicaciones.
- Desplegar la comunicación traducida en toda la Plataforma.

ANEXO II: EJEMPLO DE MODIFICACIÓN REQUERIDA PARA USAR ARCHER CON WINDOWS POWER SHELL

- El siguiente código snippet toma la versión de Archer.

```
$api_url = $base_url + "/api/core/system/applicationinfo/version"

$results = Invoke-RestMethod -Method POST -Uri $api_url -Headers $headersGET -ContentType "application/json" -WebSession $sess

$version = $results.RequestedObject.Version
```

- Actualizar un registro de contenido utilizando como identificador de contenido un fragmento ejemplo. El segundo valor HTML se comenta como un ejemplo, los valores reales no pueden divulgarse.

```
##########################################################################################################################

# UPDATE a Content Record using the Content Id created above.

#   Demo a HTML value converted to JSON and used for the update.

#     191 = Application Level Id

#    13867 = Text field

#    13868 = Text Area field (html)

##########################################################################################################################

try {

   $html = ConvertTo-Json(

      '<p>This is a description that contains HTML content with different styles,

      <strong><span style="color: #ff0000;">COLORS</span></strong>,

      <span style="font-family: comic sans ms,sans-serif;">This is COMIC SANS,

      <em><span style="font-size: 14pt;">font </span></em></span><span style="font-size: 24pt;">sizes</span>.
```

```
    <span style="background-color: #ffff00;">This is highlighted.</span></p>

    <p>My bullet points:</p> <ul> <li>Point 1</li> <li>Point 2</li> </ul>

    <p><img src="https://community.rsa.com/resources/images/palette-1004/RSA-Link_logo.png" alt="RSA Link" width="155" height="60" /></p>')

  # This HTML is a series of links to folder, files, or website.

  #$html = ConvertTo-Json(

  #    '<p><a href="file://ServerName/Share/FolderName" target="_blank">Click here to access it''s network share folder</a></p>

  #                  <p><a href="file://ServerName/Share/FolderName/MyTextFile.txt" target="_blank">Text File</a></p>

  #                                                                                  <p><a href="file://ServerName/Share/FolderName/File%20Name%20with%20spaces.pdf" target="_blank">PDF File</a></p>

  #                                                                                  <p><a href="https://knowledge.rsasecurity.com/scolcms/knowledge.aspx?solution=a64501" target="_blank">Archer Knowledge Base Article on SCOL</a></p>')

  # Replace some escaped values back to its friendly character for display.

  $html = $html.Replace("\u003c","<")

  $html = $html.Replace("\u003e",">")


  $api_url = $base_url + "/api/core/content"

  $body =

    '{"Content": {"Id": ' + $content_id + ', "LevelId": 191, "FieldContents": {

     "13867": {"Type": 1, "Value": "Name updated via REST API", "FieldId": 13867}

    ,"13868": {"Type": 1, "Value": ' + $html + ', "FieldId": 13868}

    }}}'

  $results = Invoke-RestMethod -Method PUT -Uri $api_url -Body $body -Headers $headers -ContentType "application/json" -WebSession $sess
```

```
    if ($results.IsSuccessful -and $results.ValidationMessages.count -eq 0) {
        $results
    }
    else {
        $results.ValidationMessages
    }
}
catch { $_.Exception|Format-List -Force }
finally { $results = $null }
```

ANEXO III: DESARROLLO BIA

- Ejemplo de desarrollo de BIA.

Index	Question	Answer	Risk Matrix Value	Help	Explanation
1	Resiliency Factor	Resiliency Factor	Resiliency Factor	Resiliency Factor	Resiliency Factor
1a	**Maximum Tolerable Period of Disruption (MTPD):** How long can this process be unavailable before significantly impacting the business?	1 hour	5	How long can the process operate before Cargill starts to suffer financial or operational losses.	This is the RTO for the process.
		24 Hours	4		
		72 Hours (3 Days)	3		
		7 Days	2		
		> 7 Days	1		
1b	alternate procedure exist if the technology or workspace which support this process is unavailable?	Yes	1	Has the process got a manual back up?	Is a manual process documented and in place that will allow this process to continue should it fail.
		No	5		
		**If no then do not asnwer 1c, 1d, 1e and 1f.			
1c	How long can the alternate procedure be performed?	1 hour	5	If a manual process exists how long can it be used.	How long can this procedure be run.
		24 Hours	4		
		72 Hours (3 Days)	3		
		7 Days	2		
		> 7 Days	1		
1d	Will there be an additional time or cost in doing the alternate procedure?	Yes	1	Will the implementation of a manual process cause an increase in operation cost.	
		No	5		
1e	Time (Hours/Person/Day):	<1 hour	1		
		2 - 4 hours	2		
		5 - 8 hours	3		
		9 - 11 hours	4		
		12 +	5		
1f	What is the cost of using the alternative procedure for this process? (USD per day.)	<10,000 USD	1		
		10,000 - 100,000 USD	2		
		100,000 - 200,000 USD	3		
		200,000 - 500,000 USD	4		
		500,000+ USD	5		
2	RTO	RTO	RTO	RTO	RTO
2a	**Recovery Point Objective (RPO):** If the technology supporting this process fails, how much data loss is acceptable?	7 Minutes	5		
		4 Hours	4		
		24 Hours	3		
		>24 Hours	2		
		48 Hours	1		
		>48 Hours	1		
3	Employee Factor	Employees Factor	Employees Factor	Employees Factor	Employees Factor
3a	What is the effort involved in returning to normal operations after this process has been recovered/restored?	There will be no effort in returning to normal operation once the product is available or service is restored	1	Use this scale to best describe what the effect on employees will be to return to normal business operations. When deciding this keep in mind that normal operation hours or locations may not be available.	In this section the BIA is trying to discovery what impact to staffing resumption of the process would require.
		There will be a few hours of extra work that could be handled within a normal business day	2		
		There will be work outside normal business hours, extra shifts, etc... in order to catch up. Can be completed within a week	3		
		There will be significant work outside of normal business hours. It may take up to a month to being production back up to scale.	4		
		Returning to normal operation will be difficult, require a massive amount of effort to achieve or may not be possible at all.	5		
3b	How many employees perform or depend on this process?	<10	1	This scale described the number of employees unable to perform normal business operations.	How many employees will be affected by the loss of a process.
		11 - 49	2		
		50 - 250	3		
		250 - 500	4		
		500+	5		
3c	Could the unavailability of this process increase the risk of injury or loss of life to employees or customers?	Yes	5	Would the loss of a process increase the likelihood of a serious accident resulting in injury or death.	How will the loss of this process affect H&S.
		No	1		

4	Obligation Factor	Obligation Factor	Obligation Factor	Obligation Factor	Obligation Factor
4a	Would the business fail to comply with or be unable to meet its regulatory obligations if this process cannot be performed?	Yes	5	Would the resulting loss of a process cause a breach in local or international regulation obligations.	Ascertain if ANY regulatory obligations are breached. At this point we do not need to know what only if there are any.
		No	1		
		** If YES answer 4b, if NO ignore 4b			
4e	Estimate penalties or fines that would be incurred.	<10,000 USD	1	What would be the impact in terms of fines and penalties be.	How much would the company stand to loose if regulation were not met. This could be any regulatory board.
		10,000 - 100,000 USD	2		
		100,000 - 200,000 USD	3		
		200,000 - 500,000 USD	4		
		500,000+ USD	5		
4b	Would the business fail to comply with or be unable to meet its contractual obligations if this process cannot be performed?	Yes	5		
		No	1		
		** If YES answer 4e, if NO ignore 4e			
4f	Estimate penalties or fines that would be incurred.	<10,000 USD	1	What would be the impact in terms of fines and penalties be.	How much would the company stand to loose if regulation were not met. This could be any regulatory board.
		10,000 - 100,000 USD	2		
		100,000 - 200,000 USD	3		
		200,000 - 500,000 USD	4		
		500,000+ USD	5		
4c	Does this process provide information that generates a report to Cargill Corporate?decisions?	Yes	5	This free text field is for a short description of the regulations that may be breached.	List any regulations that may be breached. If necessary the file names of the supporting documents that are attached or shown in the BCP/DRP.
		No	1		
4d	Would the loss or unavailability of this process cause a significant impact to management control or affect the ability for management to make appropriate decisions?	Yes	5		
		No	1		
7	**Financial Factor**	**Financial Factor**	**Financial Factor**	**Financial Factor**	**Financial Factor**
5a	Daily Lost Revenue	<10,000 USD	1	In every 24 hour period including weekends how much would your business stand to loose in revenue.	Daily lost revenue is the total of products not being shipped, produced or spoiling.
		10,000 - 100,000 USD	2		
		100,000 - 200,000 USD	3		
		200,000 - 500,000 USD	4		
		500,000+ USD	5		
5b	Daily Delayed Revenue	<10,000 USD	1	In every 24 hour period how much revenue stands to be delayed. This could be due to items not being shipped to cheques being delayed.	Delays in shipping, invoicing or crediting accounts may impact your business. What will the total amount of this loss be.
		10,000 - 100,000 USD	2		
		100,000 - 200,000 USD	3		
		200,000 - 500,000 USD	4		
		500,000+ USD	5		
5c	Additional operating cost?	<10,000 USD	1	In every 24 hour period will there be additional costs incurred if normal operations cannot be carried out.	What additional operating costs will be incurred due to non standard operations or loss of a process. This is not designed to show the loss but the additional cost of trying to meet your normal operations.
		10,000 - 100,000 USD	2		
		100,000 - 200,000 USD	3		
		200,000 - 500,000 USD	4		
		500,000+ USD	5		
8	**Competitive Factor**	**Competitive Factor**	**Competitive Factor**	**Competitive Factor**	**Competitive Factor**
8a	How many customers do you currently have for your products / services?	<10	1		
		11 - 49	2		
		50 - 249	3		
		250 - 499	4		
		500+	5		
8b	What percentage of your customers would be affected by the loss of this service?	<10%	1		
		11 - 25%	3		
		26 - 50%	4		
		<50%	5		
8c	How long will customers wait before seeking an alternative source for your product / service?	>7	1		
		4 - 7 Days	2		
		1 - 3 Days	3		
		<24	5		
8d	What percentage of your customers will return to your product / service?	<10%	1		
		11 - 25%	3		
		26 - 50%	4		
		<50%	5		

9	Reputation Factor	Reputation Factor	Reputation Factor	Reputation Factor	Reputation Factor
9a	Use the following scale for identifying the impact to your reputation as a result of the loss of this product or service. NOTE: where it says "customers" please also consider other stakeholders such as: Suppliers, Capital Providers, Government Agencies, etc...	1=There will be no impact to reputation.	1		
		2=There will be **some** impact to reputation, current customers will not leave, but it will affect the ability for acquiring new customers.	2		
		3=There is a moderate impact to reputation. Some Customers will stop using the product/service. It will affect the ability for acquiring new customers. Loss will be recoverable after service/product is restored.	3		
		4=There is a significant impact to reputation. Customers will stop using the product/service. It will affect the ability for acquiring new customers. Loss is recoverable, but will take some time and effort.	4		
		5=There is a critical impact to reputation. Customers will stop using the product/service. It will affect the ability for acquiring new customers. Loss is permanent or will take significant time and effort to recover.	5		

ANEXO IV: LISTA DE ACRÓNIMOS

BCM	: BUSINESS CONTINUITY MANAGEMENT
BCP	: BUSINESS CONTINUITY PLANNING
BIA	: BUSINESS IMPACT ANALYSIS
BRM	: BUSINESS RISK MANAGER
BRP	: BUSINESS REENGINEERING PROCESS
BU	: BUSINESS UNIT
BUIA	: BUSINESS UNIT IMPACT ANALYSIS
CEO	: CHIEF EXECUTIVE OFFICER
CIP	: CARGILL INFORMATION PROTECTION
CMC	: CRISIS MANAGEMENT COMMITTEE
CMP	: CRISIS MANAGEMENT PLANNING
DRP	: DISASTER RECOVERY PLANNING
EPS	: EARNING PER SHARE
IDS	: INSTRUSION DETECTION SYSTEM
IP	: IMFORMATION PROTECTION
IT	: INFORMATION TECHNOLOGY
ITIL	: IT INFRASTRUCTURE LIBRARY
ITM	: IT MANAGER
ITSB	: IT SERVICE BUSINESS
LA	: LATIN AMERICA
OSP	: OUTSIDE SERVICE PROVIDER
RA	: RISK ANALYST
RCC	: RISK AND CONTROL COORDINATOR
RM	: RESILIENCY MANAGEMENT
RPO	: RECOVERY POINT OBJETIVE
RTO	: RECOVERY TIME OBJETIVE
SAM	: SOFTWARE ASSET MANAGEMENT
SI	: STRATEGIC INTENT
SME	: SUBJECT MATTER EXPERT
SRCC	: SITE RISK AND CONTROL COORDINATOR
SSC	: SHARED SERVICE CENTER
TGRC	: TECHNOLOGY GOVERNANCE RISK AND CONTROL
TR&C	: TECHNOLOGY RISK AND CONTROL
TRA	: TECHNOLOGY RISK ANALYST
TRCC	: TECHNOLOGY RISK COORDINATOR
TRCM	: TECHNOLOGY RISK AND CONTROL MANAGER

ANEXO V: ÍNDICE DE FIGURAS Y TABLAS

FIGURA	PÁGINA
Figura 1. Forma en que mitiga la empresa el riesgo respectivo	8 y 9
Figura 2. Horizonte hacia donde se dirige TGRC.	10
Figura 3. Plataforma Global de TGRC	13
Figura 4. Resumen de Roles del autor, con excepción de los que poseen rango de *Manager donde compartía funciones con Javier Fantini (IT Manager para Beef Argentina) en lo que respecta a TGRC.*	13 y 14
Figura 5. Marco del conjunto de políticas bases.	21
Figura 6. Archer, Gestión de Amenazas.	26
Figura 7. Componentes del proceso de comunicación.	34
Figura 8. Ecosistema Archer.	39
Figura 9. Logueo en Archer.	42
Figura 9. Ejemplo: Módulo Gestión de Incidentes.	43
Figura 10. Ejemplo: Módulo Gestión de Amenazas Detectadas	44
Figura 11. Ejemplo: Módulo Carga de Proceso.	44
Figura 12. Árbol de registros dentro de Archer.	46
Figura 13. Principales desafíos en la empresa	48
Figura 14. Nuevos roles para direcciones de las políticas entregables del Centro de Coordinación de Riesgos (RCC).	60
Figura 15. Traducción y Despliegue de conocimientos.	67
Figura 16. Nuevos roles TRCC para direcciones de las políticas de TGRC.	69
Figura 17. Centro de Gestión de amenazas en Archer.	73
Figura 18. Marco de Resiliencia de la Unidad de Negocio	78
Figura 19. Estructura del BCP.	92
TABLA	**PÁGINA**
Tabla 1. Despliegue propuesto por TGRC a nivel mundial.	15
Tabla 2. Calificación utilizada.	25
Tabla 3. Aspectos evaluados por las métricas	31
Tabla 3. Reporte mensual de métricas.	32
Tabla 4. Comparación de métricas entre diferentes BU.	33
Tabla 5. Rango de calificaciones	33
Tabla 6. Definición de roles.	36
Tabla 7. Software recolector de datos.	36
Tabla 8. Procesos Preestablecidos por Tartan.	52, 53, 54 y 55
Tabla 9. Tecnologías usadas por el Proceso.	55
Tabla 10. Relación Actividad – KRA para RCC.	65
Tabla 11. Relación Actividad – KRA para TRCC.	70 y 71
Tabla 12. Informe de Archer utilizado como coordinación.	74
Tabla 13. Calificación utilizada.	74

ANEXO VI: BIBLIOGRAFÍA

Enfoque:

[1] http://www.sustainablebrands.com/news_and_views/communications/defining-sustainability-process-strategy-focus

Políticas – Harvard:

[2]http://hwpi.harvard.edu/files/provost/files/policy_on_access_to_electronic_information.pdf

Misión y Visión:

[3] http://open.lib.umn.edu/principlesmanagement/chapter/4-3-the-roles-of-mission-vision-and-values

[4] Bart, C. K., & Baetz, M. C. (1998). The relationship between mission statements and firm performance: An exploratory study. Journal of Management Studies, 35, 823–853

[5] Bart, C. K., Bontis, N., & Taggar, S. (2001). A model of the impact of mission statements on firm performance. Management Decision, 39(1), 19–35

[6] Hamel, G., & Prahalad, C. K. (1993, March–April). Strategy as stretch and leverage. Harvard Business Review, 75–84

[7] Ogilvy, Retrieved October 27, 2008, from http://www.ogilvy.com/o_mather

[8] Starbucks, retrieved October 27, 2008, from http://www.starbucks.com/aboutus

[9] Toyota, retrieved October 27, 2008, from http://www.toyota.co.jp/en/vision/philosophy

[10] Walmart, retrieved October 27, 2008, from http://www.walmart.com

Tartan

[11]Universidad de Minnesota: http://www.misrc.umn.edu/seminars/2010-04-30/

Métricas:

[12] http://www.suranacollege.edu.in/surana-pg/pdf/mca/Process-And-Project-Metrics.pdf

[13] https://www.projectmanager.com/blog/project-performance-metrics

[14] Harvard Business: https://hbr.org/2012/10/the-true-measures-of-success

Varios:

[15] BUSINESS PROCESS DEFINITION
Umit S Bititci and Daniel Muir, DMEM, University of Strathclyde, Glasgow, UK

[16] BRP LIFECCYCLE, Business Process Reengineering by Lampathaki F., Koussouris S., Psarras J. Universidad de Atenas- Grecia
[17] Enhancing Customer Value Through 'Top-Down' Business Process Management - Cognizant
[18] Business Case Essentials - Marty Schmidt
[19] The evolution of business resiliency management - IBM
[20] How Resilience Works, by Diane Coutu - Harvard
[21] https://sph.tulane.edu/certificate-disaster-management-and-resilience Tulane University - New Orleans, EE. UU
[22] B. Miroslav. The risk assessment of information system security. University of Zagreb, Faculty of Organization and Informatics, Varašdin, Croatia
[23] Principles of Management- Charles Hill, Steven McShane
[24] Safety and health for engineers - Roger L. Brauer
[25] Governance, Risk and Compliance
[26] Policy Management: Methods and Tools