Polo del Conocimiento

Pol. Con. (Edición núm. 41) Vol. 5, No 01
Enero 2019, pp. 69-86
ISSN: 2550 - 682X
DOI: 10.23857/pc.v5i01.1212

Plan de recuperación ante desastres tecnológicos en el Grupo Industrial Graiman

Technological disaster recovery plan at Grupo Industrial Graiman

Plano tecnológico de recuperação de desastres no Grupo Industrial Graiman

Julio Esteban Ramos-Medina [I]
esjuramos@hotmail.com
https://orcid.org/0000-0001-9415-4059

Víctor Manuel Paliz-Osorio [II]
victor.paliz@ucacue.edu.ec
https://orcid.org/0000-0002-9218-3355

Correspondencia: esjuramos@hotmail.com

Ciencias de las ingenierías
Artículo de investigación

*__Recibido:__ 24 de noviembre de 2019 *__Aceptado:__ 28 diciembre de 2019 * __Publicado:__ 17 de enero 2020

I. Ingeniero de Sistemas, Jefatura de Posgrados Universidad Católica de Cuenca, Cuenca, Ecuador.
II. Magíster en Informática, Docente, Jefatura de Posgrados Universidad Católica de Cuenca, Cuenca, Ecuador

Resumen

Existen ciertos servicios que se encuentran operando en la fábrica del GIG, los cuales requieren atención puesto que alojan servicios e infraestructura crítica para la operación del negocio. Se pretende resolver la problemática planteada mediante el desarrollo de un plan de recuperación ante desastres tecnológicos en el GIG para levantar en el menor tiempo posible los servicios y activos tecnológicos de la organización. Es sustento de ocupación y de debilidad el hecho cierto de no poseer el control total sobre la infraestructura de la organización y ante las constantes vulnerabilidades, amenazas y riesgos, como: desastres naturales, atentados, robos, ataques informáticos o errores humanos, etc., que surgen diariamente. Por tanto, la organización se encuentra expuesta a la pérdida de la continuidad del servicio o interrupciones no programadas, lo cual podría generar serios problemas financieros, Para realizar el análisis de riesgos se tomó como marco de referencia la metodología Magerit. Antes de empezar el desarrollo del análisis de riesgos, es necesario conocer la terminología que se maneja en Magerit. existe una brecha muy grande entre lo que el negocio espera de la recuperación de servicios e infraestructura, con respecto al tiempo objetivo, y, la cantidad de datos tolerantes a pérdida versus lo que el departamento de TICS puede ofrecer actualmente con las herramientas tecnológicas que se posee. Sería necesario realizar una difusión de los procesos y activos críticos identificados en el análisis de impacto en el negocio para mantener la continuidad del negocio asegurando la participación y colaboración de todos los involucrados.

Palabras clave: plan de recuperación; negocios; tecnología; industria, servicios

Abstract

There are certain services that are operating in the GIG factory, which require attention since they host critical services and infrastructure for the operation of the business. It is intended to solve the problem posed by developing a recovery plan for technological disasters in the GIG to raise the technological services and assets of the organization in the shortest possible time. The fact of not possessing total control over the infrastructure of the organization and the constant vulnerabilities, threats and risks, such as: natural disasters, attacks, robberies, computer attacks or human errors, etc., is a source of occupation and weakness. that arise daily. Therefore, the organization is exposed to the loss of service continuity or unscheduled interruptions, which could generate serious

financial problems. To carry out the risk analysis, the Magerit methodology was used as a reference framework. Before beginning the development of risk analysis, it is necessary to know the terminology that is handled in Magerit. There is a very large gap between what the business expects from the recovery of services and infrastructure, with respect to the target time, and, the amount of data tolerant to loss versus what the TICS department can currently offer with the technological tools that are available. has. It would be necessary to disseminate the processes and critical assets identified in the business impact analysis to maintain business continuity ensuring the participation and collaboration of all involved.

Keywords: recovery plan; business; technology; industry, services

Resumo

Existem certos serviços que estão operando na fábrica da GIG, que requerem atenção, pois hospedam serviços e infraestrutura essenciais para a operação dos negócios. Pretende-se resolver o problema proposto, desenvolvendo um plano de recuperação de desastres tecnológicos no GIG para elevar os serviços e ativos tecnológicos da organização no menor tempo possível. O fato de não possuir controle total sobre a infraestrutura da organização e as constantes vulnerabilidades, ameaças e riscos, como: desastres naturais, ataques, assaltos, ataques a computadores ou erros humanos, etc., é a base da ocupação e da fraqueza. que surgem diariamente. Portanto, a organização está exposta à perda da continuidade do serviço ou a interrupções não programadas, o que pode gerar sérios problemas financeiros. Para realizar a análise de risco, a metodologia Magerit foi usada como estrutura de referência. Antes de iniciar o desenvolvimento da análise de risco, é necessário conhecer a terminologia tratada no Magerit. existe uma lacuna muito grande entre o que os negócios esperam da recuperação de serviços e infraestrutura, com relação ao tempo objetivo e a quantidade de dados tolerantes a perdas versus o que o departamento TICS pode oferecer atualmente com as ferramentas tecnológicas disponíveis. possui Seria necessário disseminar os processos e ativos críticos identificados na análise de impacto nos negócios para manter a continuidade dos negócios, garantindo a participação e colaboração de todos os envolvidos.

Palavras chave: plano de recuperação; negócios; tecnologia; indústria, serviços

Introducción

Graiman fue fundada en febrero del año 1994, con una inversión de capitales 100% ecuatorianos. Se encuentra ubicada estratégicamente en Cuenca, Ecuador, ciudad cerámica por excelencia; región que en sus alrededores alberga suelos con las más ricas arcillas, feldespatos y caolines, que han hecho de esta, un lugar privilegiado para el desarrollo de la industria cerámica. Todas las empresas y organizaciones se encuentran expuestas a situaciones de riesgo, como: desastres naturales, atentados terroristas, robos, ataques informáticos, errores humanos, conmoción social, etc., que pueden afectar a la continuidad del negocio y el funcionamiento normal de la organización. Es una tarea importante conocer claramente los riesgos y tener la capacidad para afrontarlos.

En la actualidad el GIG mantiene su infraestructura de misión crítica en una nube privada con un proveedor externo, el centro de datos se encuentra localizado en la ciudad de Quito. Se mantiene un contrato con el modelo de infraestructura como servicio Iass (Infraestructura como servicio). El GIG al no poseer el control sobre la infraestructura evidencia un problema potencial de pérdida de servicio, estas acciones generan incertidumbre en la empresa puesto que significan pérdidas financieras y causan problemas a nivel estratégico y de prestigio.

Adicionalmente, existen ciertos servicios que se encuentran operando en la fábrica del GIG los cuales requieren atención puesto que alojan servicios e infraestructura crítica para la operación del negocio. La consecución adecuada de este trabajo ayudará a resolver la problemática planteada mediante el desarrollo de un plan de recuperación ante desastres tecnológicos en el GIG para levantar en el menor tiempo posible los servicios y activos tecnológicos de la organización.

Desarrollo

Materiales y métodos

Es sustento de ocupación y de debilidad el hecho cierto de no poseer el control total sobre la infraestructura de la organización y ante las constantes vulnerabilidades, amenazas y riesgos, como: desastres naturales, atentados, robos, ataques informáticos o errores humanos, etc., que surgen diariamente. Por tanto, la organización se encuentra expuesta a la pérdida de la continuidad del servicio o interrupciones no programadas, lo cual podría generar serios problemas financieros, estratégicos, operativos y de prestigio, por interrupciones no planificadas.

Bajo este contexto el grupo industrial Graiman se encuentra con la necesidad de realizar un plan de recuperación ante desastres, con el fin de mantener la rentabilidad de la empresa y garantizar la continuidad del servicio, al contar con una recuperación ordenada, eficiente y efectiva de los servicios vitales de la organización.

La etapa de análisis de impacto en el negocio permite:

- Identificar con claridad los servicios de misión crítica para la organización y a su vez permite analizar el nivel de impacto que puede tener una interrupción de servicio.
- Tener una visión amplia del impacto operativo y financiero sobre los servicios considerados de misión crítica para la organización.

Establecer los tiempos de recuperación ante una posible interrupción de los servicios críticos.

Metodología

Para el desarrollo del presente trabajo se realizó una investigación de campo, cualitativa-cuantitativa junto con un análisis de la situación actual de la empresa para identificar los posibles problemas, amenazas, riesgos y vulnerabilidades. Se efectuaron diversos análisis de la situación actual en la empresa para poder establecer una adecuada planificación de contingencias. Fueron necesarias varias entrevistas y reuniones con diferentes departamentos de la organización para lograr un mayor entendimiento del impacto que tendría la pérdida de la continuidad del negocio y la afectación a nivel financiero, estratégico y operativo que supondría este problema.

Se utilizó una técnica de investigación: Entrevistas: Se realizaron reuniones con varios departamentos de la organización, con el fin de llegar a un entendimiento claro de la problemática y establecer las mejores soluciones.

Universo de estudio y tratamiento muestral.

El tamaño de la muestra fue mediante el estudio de grupo, para seleccionar los elementos de la muestra se utilizó un muestreo probabilístico, en donde se capturó al azar a ciertos empleados tomando como enfoque las áreas de solución y desarrollo de la investigación, específicamente del departamento de TIC, se desarrolló un análisis cualitativo de los resultados. Por lo que se tomaron

60 personas con representación de los departamentos tal como se observa en la tabla 2, que a continuación se presenta:

Tabla 2. Muestra entrevistas en GIG

DEPARTAMENTO	PERSONAS	PORCENTAJE
MANUFACTURA	15	**25,00%**
LOGÍSTICA	6	**10,00%**
TRANSPORTE	10	**16,67%**
COMERCIAL	6	**10,00%**
FINANZAS	6	**10,00%**
COMPRAS	6	**10,00%**
RECURSOS HUMANOS	5	**8,33%**
TECNOLOGÍAS DE LA INFORMACIÓN	6	**10,00%**
TOTALES	**60**	**100**

Fuente: GIG. **Elaboración** propia (2019)

Resultados

Debido a la dependencia que existe entre la organización y los servicios e infraestructura tecnológica, la presencia de una interrupción no programada conlleva a hablar del concepto de continuidad del negocio, cuyo objetivo es minimizar la probabilidad e impacto de posibles pérdidas de servicio. La siguiente tabla indica el resultado de la cantidad de tiempo tolerable de indisponibilidad de los servicios TIC por parte de los usuarios:

RESULTADOS RTO											
		100%	5m	0m	1h	h	4h	8h	4h	h	72h
#	Servicios TIC	1	2	3	4		6	7	8		10
1	ERP	X									
2	INTERNET		X								
3	FICE365(OFIMATICA, CORREO, AREPOINT, TEAMS, ONE DRIVE)	X									
4	TELEFONIA			X							
5	NOMINA				X						
6	SHINE			X							
7	NAS		X								
8	FILESERVER	X									
9	IMPRESIÓN		X								
10	NAS		X								
11	ONLY CONTROL	X									
12	COMPERS							X			
13	RPA				X						
14	Adaptive								X		
15	RP3				X						
16	SMPROG		X								
17	ENLACES DATOS		X								
18	UPS		X								
19	TIME CONTROL						X				
20	RELOJ MARCACION	X									
21	SPYRAL				X						
22	DRIVING						X				

23	QLIKVIEW						X					

Tabla 3 Resultados RTO del negocio Fuente: GIG

Ante situaciones de riesgo de diversa índole, como una simple falta de energía eléctrica, por ejemplo se puede generar grados de indisponibilidad de los servicios de la organización en términos de tiempo y en dependencia de los servicios de que se trate, mientras más se corresponda con servicios de equipos, servicios on line y servicios de oficina y diversas aristas administrativas e informáticas mayor indisponibilidad habrá para la atención efectiva de este tipo de servicios, lo cual puede generar riesgos, e impacto de pérdida en la administración. Por su parte, la siguiente tabla indica el resultado de la cantidad de datos tolerables de posible pérdida cuando exista una interrupción de los servicios desde el lado del negocio.

RESULTADOS RPO

		00%	30m	2h	4h	8h	4h	72h
	Servicios TIC	1	2	3	4	5	6	7
1	ERP	X						
2	INTERNET							
3	E365(OFIMATICA, CORREO, AREPOINT, TEAMS, ONE DRIVE)	X						
4	TELEFONIA							
5	NOMINA	X						
6	SHINE				X			
7	NAS	X						
8	FILESERVER	X						
9	IMPRESIÓN							
10	NAS	X						
11	ONLY CONTROL	X						
12	COMPERS							X
13	RPA			X				
14	Adaptive						X	
15	RP3						X	
16	SMPROG		X					
17	ENLACES DATOS							
18	UPS							
19	TIME CONTROL	X						
20	RELOJ MARCACION							
21	SPYRAL		X					
22	DRIVING						X	
23	QLIKVIEW			X				

Figura 1 Resultados RPO del negocio Fuente: GIG

Los resultados con respecto al punto objetivo de recuperación (RPO), desde el lado del departamento de TIC, se muestran en la siguiente tabla:

Resultados estimación TICS para RPO

		100%	0m	1h	2h	4h	8h	4h	0
	DATOS	1	2	3	4	5	6	7	8
1	ERP			X					
2	INTERNET								
3	ICE365(OFIMATICA, CORREO, SHAREPOINT, TEAMS, ONE DRIVE)		X						

4	TELEFONIA								
5	NOMINA							X	
6	SHINE							X	
7	NAS								X
8	FILESERVER								X
9	IMPRESIÓN								
10	ONLY CONTROL							X	
11	COMPERS							X	
12	RPA								X
13	Adaptive							X	
14	RP3							X	
15	SMPROG							X	
16	ENLACES DATOS								
17	UPS								
18	TIME CONTROL							X	
19	RELOJ MARCACION								
20	SPYRAL					X			
21	DRIVING								X
22	QLIKVIEW				X				

Figura 2 Resultados estimación TIC para RPO Fuente: GIG

La siguiente figura muestra un cuadro comparativo entre la cantidad de datos tolerables para perder que puede soportar el negocio, versus la cantidad de datos que el departamento de TIC puede restaurar con las herramientas tecnológicas que poseen actualmente.

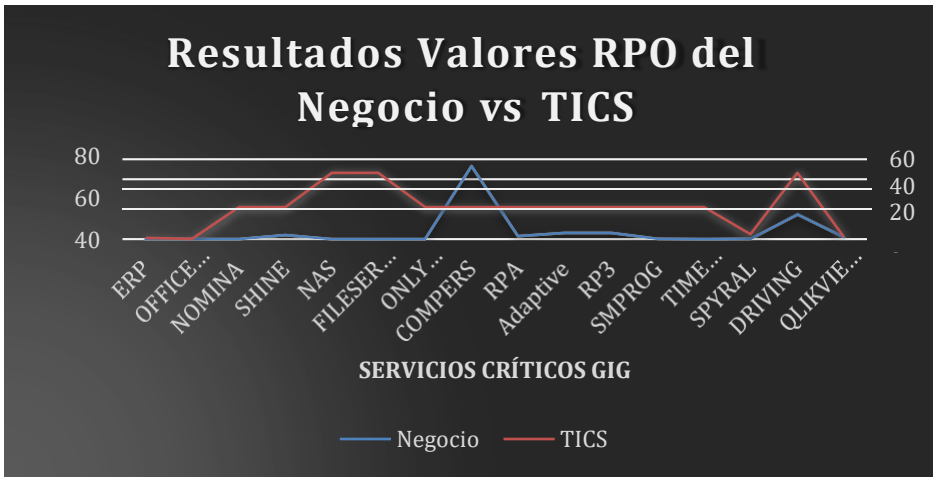


Figura 3 Resultados valores RPO del Negocio vs TICS Fuente: GIG

La siguiente figura indica el resultado del análisis de riesgos en el cual se puede identificar que el 11% de los activos que están catalogados como críticos necesitan una mitigación urgente, mientras que el 89% se encuentran como un riesgo aceptable por la organización.

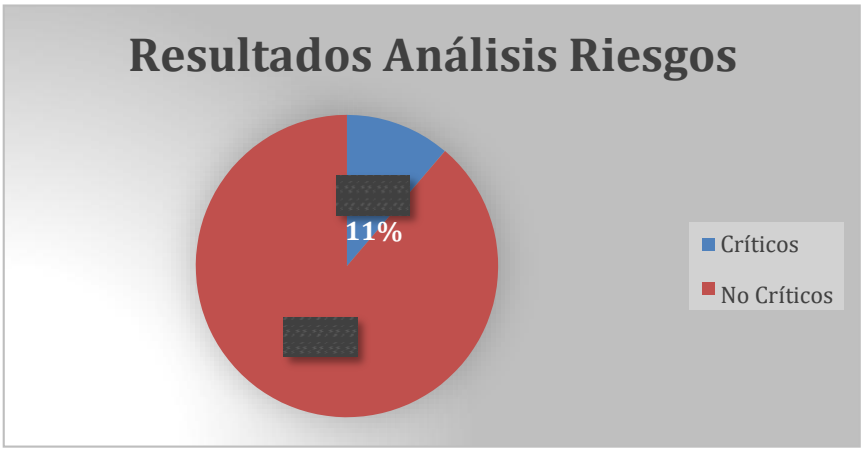


Figura 10 Resultados del análisis de riesgos Fuente: GIG

Plan de recuperación ante desastres tecnológicos (DRP)

Nro.	ACTIVIDAD	ROL ASOCIADO A ACTIVIDAD
1	Identificar la gravedad de la contingencia y estimar su impacto aplicando una visión general.	Establecimiento de daños, Jefe de Recuperación
2	Declarar la situación de contingencia y notificar a Gerencia General.	Jefe de Recuperación, Administración de instalación y logística
3	Reunir a los diferentes miembros del ER requeridos para iniciar la recuperación del procesamiento. Reasignar los roles que sean necesarios.	Jefe de Recuperación
4	Evaluar y precisar la severidad del daño en términos operativos, así como también el tiempo estimado más cercano de recuperación (evaluar qué sistemas se afectaron, qué equipos han quedado inservibles, cuales se pueden recuperar, y en cuanto tiempo, etc.). Informar a la Gerencia General y Direcciones relacionadas.	Jefe de Recuperación, Administración de instalación y logística
5	Revisar rápidamente el Plan y confirmar o modificar la secuencia y prioridad de las actividades, dependiendo de las consecuencias del desastre, y de los recursos disponibles.	Jefe de Recuperación

Pol. Con. (Edición núm. 41) Vol. 5, No 01, enero 2020, pp.69-86, ISSN: 2550 - 682X

6	Distribuir al ER copias del Plan y listas de tareas asignadas durante la actividad anterior.	Jefe de Recuperación
7	Notificar a los proveedores de hardware, software, base de datos y servicios.	Jefe de Recuperación
8	Evaluar simultáneamente la posibilidad de contar con un procesamiento alterno temporal para las aplicaciones críticas que no se podrán recuperar rápidamente. Esto obliga a usar el plan de la continuidad del negocio, si existe, o a improvisar urgentemente uno durante esta contingencia.	Administración de instalación y logística, Software de aplicaciones

Análisis de impacto en el negocio (BIA business impact analysis).

La información del BIA fue obtenida mediante entrevistas con direcciones, gerencias y jefaturas de las distintas áreas, que se muestran en la tabla 1, la cual se presenta a continuación:

Tabla 1. Áreas de entrevistas para BIA

ÁREAS
Ma Manufactura
L Logística
Transporte
Comercial
Finanzas
Compras
Recursos humanos
Tecnologías de la información

Fuente: Datos proporcionados por la gerencia de GIG al 2019.**Elaboración** propia (2019)

Para determinar el tiempo de recuperación objetiva (RTO recovery time objective) tolerable por parte del negocio y el tiempo de recuperación objetiva (RPO recovery point objective), es decir, la cantidad tolerable de pérdida de datos para el negocio, se siguió de acuerdo con las figuras 1 y 2, adaptadas lo más cercano a las necesidades del negocio:

TABLA PARA ESTIMAR EL RTO	
VALOR	**DESCRIPCIÓN**
1	La actividad o el proceso requiere alta disponibilidad (100%).
2	La actividad o el proceso requiere disponibilidad hasta 15 minutos.
3	La actividad o el proceso requiere disponibilidad hasta 30 minutos.
4	La actividad o el proceso requiere disponibilidad hasta 60 minutos.
5	La actividad o el proceso requiere disponibilidad hasta dos horas.
6	La actividad o el proceso requiere disponibilidad hasta 4 horas
7	La actividad o el proceso no puede estar interrumpida más de 8 horas.
8	La actividad o el proceso no puede estar interrumpida más de 24 horas.
9	La actividad o el proceso no puede estar interrumpida más de 72 horas.
10	Otros requisitos menos restrictivos que los indicados previamente.

Figura 1 Tabla para estimar el RTO Fuente: GIG

TABLA PARA ESTIMAR EL RPO	
VALOR	**DESCRIPCIÓN**
1	La actividad o el proceso requiere disponer del 100% de los datos.
2	La actividad o el proceso tolera el retraso de los datos generados o modificados en los últimos 30 minutos o menos
3	La actividad o el proceso tolera el retraso de los datos generados o modificados en las dos últimas horas
4	La actividad o el proceso tolera el retraso de los datos generados o modificados en las últimas 4 horas.
5	La actividad o el proceso tolera el retraso de los datos generados o modificados en las últimas 8 horas.
6	La actividad o el proceso tolera el retraso de los datos generados o modificados en las últimas 24 horas.
7	Otros requisitos menos restrictivos que los indicados previamente.

Figura 2 Tabla para estimar el RPO Fuente: GIG

Impacto financiero

El GIG basa su giro de negocio en las ventas y producción o manufactura, por lo cual se realizó un análisis financiero tomando como referencia estas dos áreas, para el primer caso de las ventas se tomó como parámetro un día de cada mes, comprendidos entre enero y agosto de 2019, respectivamente, donde las ventas tienen un porcentaje más alto.

		FECHAS DE VENTAS								Promedio Venta
		19/1/2019	19/2/2019	19/3/2019	19/4/2019	19/5/2019	19/6/2019	19/7/2019	19/8/2019	
PARAMETROS	1 hora	19.507,04	32.982,87	14.994,88	29.722,52	26.866,10	9.009,00	25.912,04	7.811,90	**20.850,79**
	2 horas	39.014,09	65.965,74	29.989,77	59.445,03	53.732,19	18.018,00	51.824,09	15.623,81	**41.701,59**
	4 horas	78.028,17	131.931,48	59.979,53	118.890,06	107.464,39	36.036,01	103.648,18	31.247,62	**83.403,18**
	8 horas	156.056,34	263.862,95	119.959,07	237.780,12	214.928,77	72.072,02	207.296,36	62.495,23	**166.806,36**
	1 día	468.169,02	791.588,86	359.877,20	713.340,36	644.786,32	216.216,05	621.889,07	187.485,69	**500.419,07**
	2 días	813.894,20	1.077.128,68	905.727,91	1.164.156,84	1.150.880,68	797.930,90	988.250,12	641.794,07	**942.470,43**
	3 días	1.061.173,96	1.343.504,55	1.223.264,29	1.261.215,91	1.528.335,91	1.122.659,07	1.225.691,41	983.380,77	**1.218.653,23**
	5 días	1.368.759,62	1.711.211,88	1.797.798,07	1.795.353,09	2.096.865,75	1.680.131,30	1.481.492,22	1.726.822,24	**1.707.304,27**

Figura 3 Análisis financiero de ventas Fuente: GIG

Pol. Con. (Edición núm. 41) Vol. 5, No 01, enero 2020, pp.69-86, ISSN: 2550 - 682X

Para el caso del análisis financiero de manufactura, se tomó como referencia los meses desde enero hasta agosto, y, en este caso se tomaron en cuenta todos los días laborados de cada mes. Lo cual dio cuenta de que hubo mayor entrada por ventas en los meses de febrero, marzo y mayo, esto se corrobora en los datos que refleja la siguiente figura.

	FECHAS DE PRODUCCION MANUFACTURA							
PARÁMETROS	**19/1/2019**	**19/2/2019**	**19/3/2019**	**19/4/2019**	**19/5/2019**	**19/6/2019**	**19/7/2019**	**19/8/2019**
Producción	673.428,31	870.808,07	901.766,33	844.462,19	751.949,57	746.082,04	886.022,94	801.539,19
Costo unitario	5,11	4,35	4,35	4,37	4,55	4,86	4,46	5,05
Costo producción	**3.438.831,42**	**3.785.336,92**	**3.923.808,25**	**3.689.130,16**	**3.417.888,59**	**3.622.543,04**	**3.953.024,06**	**4.047.702,70**
Días laborados	31	28	31	30	31	30	31	31

Figura 4 Análisis financiero manufactura Fuente: GIG

Análisis de riesgos.

Para realizar el análisis de riesgos se tomó como marco de referencia la metodología Magerit. Antes de empezar el desarrollo del análisis de riesgos, es necesario conocer la terminología que se maneja en Magerit, para abordar de una manera más adecuada con el marco de referencia.

Terminología.

- Activo: Componente o servicio que forma parte de una organización, el cual es susceptible a cualquier tipo de ataques.
- Amenaza: Son aquellos problemas potenciales que se relacionan con la seguridad de los activos.
- Vulnerabilidad: Es un hecho o debilidad mediante la cual una amenaza puede materializarse sobre algún activo.
- Riesgo: Se denomina a la probabilidad de que una amenaza se vuelva realidad sobre uno o más activos.
- Salvaguardas: Son aquellos mecanismos que ayudan a reducir el riesgo de acuerdo al catálogo que recomienda magerit.
- Impacto residual: Es el resultado final de la aplicación de las salvaguardas a las amenazas de los activos.

Pol. Con. (Edición núm. 41) Vol. 5, No 01, enero 2020, pp. 69-86, ISSN: 2550 - 682X

		FECHAS DE PRODUCCIÓN MANUFACTURA								Promedio Costo
		19/1/2019	19/2/2019	19/3/2019	19/4/2019	19/5/2019	19/6/2019	19/7/2019	19/8/2019	
PARÁMETROS	1 hora	4.622,09	5.632,94	5.273,94	5.123,79	4.593,94	5.031,31	5.313,20	5.440,46	5.128,96
	2 horas	9.244,17	11.265,88	10.547,87	10.247,58	9.187,87	10.062,62	10.626,41	10.880,92	10.257,92
	4 horas	18.488,34	22.531,77	21.095,74	20.495,17	18.375,75	20.125,24	21.252,82	21.761,84	20.515,83
	8 horas	23.110,43	28.164,71	26.369,68	25.618,96	22.969,68	25.156,55	26.566,02	27.202,30	25.644,79
	1 día	110.930,05	135.190,60	126.574,46	122.971,01	110.254,47	120.751,43	127.516,91	130.571,05	123.095,00
	2 días	221.860,09	270.381,21	253.148,92	245.942,01	220.508,94	241.502,87	255.033,81	261.142,11	246.190,00
	3 días	332.790,14	405.571,81	379.723,38	368.913,02	330.763,41	362.254,30	382.550,72	391.713,16	369.284,99
	5 días	554.650,23	675.953,02	632.872,30	614.855,03	551.272,35	603.757,17	637.584,53	652.855,27	615.474,99

Figura 5 Análisis financiero manufactura Fuente: GIG

Capacidad de TICS para RTO y RPO

De acuerdo con información levantada en el departamento de tecnologías de información se establecieron las capacidades reales en tiempos de recuperación objetivos. Para esa valoración se utilizó la siguiente tabla:

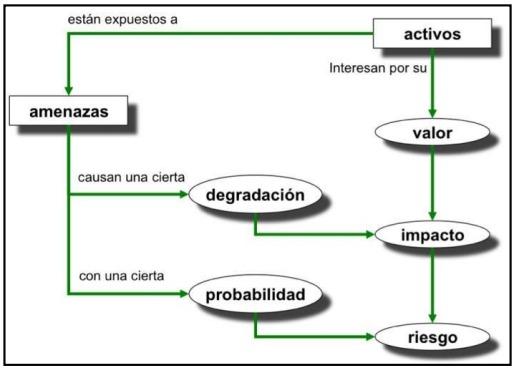
LA ESTIMACIÓN TICS PARA RTO	
VALOR	DESCRIPCIÓN
1	Los servicios o herramientas TIC poseen disponibilidad del 100%
2	osible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo de 15 minutos
3	osible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo de 30 minutos
4	osible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo de 60 minutos
5	osible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo de 2 horas
6	osible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo de 4 horas
7	osible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 8h.
8	osible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 24h.
9	osible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 72h.
10	xisten medios que garanticen la recuperación de los servicios y herramientas TIC de que dependen la actividad o el proceso en un tiempo inferior a los indicados y/o el tiempo de recuperación no está acotado.

Figura 6 Tabla estimación TICs para RTO Fuente: GIG

Riesgo residual: Son los riesgos sobrantes luego de haber aplicado las medidas de seguridad respectivas.

La siguiente figura permite entender la relación entre la terminología indicada:

Figura 7 Elementos del análisis de riesgos Fuente: Magerit V3.0 Libro de método



Identificación de los activos

Esta figura refleja cómo las amenazas puede afectar y causar degradación y riesgos de impacto en las finanzas de la organización.

Conclusiones

Se puede concluir el presente trabajo, enfocando la atención en 3 aspectos, tal como sigue a continuación: el análisis de impacto en el negocio, el análisis de riesgos y el plan de recuperación ante desastres tecnológicos. Con respecto al análisis de impacto en el negocio se puede comentar que existe una brecha muy grande entre lo que el negocio espera de la recuperación de servicios e infraestructura, con respecto al tiempo objetivo, y, la cantidad de datos tolerantes a pérdida versus lo que el departamento de TICS puede ofrecer actualmente con las herramientas tecnológicas que se posee.

Con lo referente al análisis de riesgos, existe una cantidad significativa de riesgos que deben ser mitigados para evitar cualquier indisponibilidad de servicios e infraestructura, puesto que en el análisis financiero presentado en este trabajo se ve claramente que estar sin servicio en las actividades clave de la empresa demanda una cantidad de dinero importante.

Sería necesario realizar una difusión de los procesos y activos críticos identificados en el análisis de impacto en el negocio para mantener la continuidad del negocio asegurando la participación y colaboración de todos los involucrados.

Es importante realizar un seguimiento a la mitigación de los riesgos identificados y efectuar constantemente una actualización del análisis de riesgos, para identificar la infraestructura que es soportada por los servicios de TICS.

Se deben realizar tareas de revisión, actualización, pruebas y mantenimiento de los planes de continuidad de infraestructura tecnológica al menos una vez por año.

Términos y definiciones

- DRP: Plan de recuperación ante desastres (disaster recovery plan)
- GIG: Grupo Industrial Graiman
- TICS: Tecnologías de información y comunicación
- RTO: Tiempo objetivo de recuperación (recovery time objective)
- RPO: Punto de recuperación objetiva (recovery point objective)
- MTD: Tiempo de inactividad tolerable (Maximum Tolerable Downtime)
- BIA: Análisis de impacto en el negocio (business impact analysis) BCP: Plan de continuidad del negocio (business continuity plan) FailOver: Conmutación por error
- Base de datos StandBy: Base de datos de espera

Referencias

1. Angel, S. (2015). Modelo de gestión de continuidad de infraestructura tecnológica para la operación de servicios de TI en empresas financieras sobre la base de las normas ISO 22301 e ISO 27001. Aplicación a un caso de estudio. Repositorio Digital Universidad De Las Américas.
2. Angela, S. (2016). DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL DEPARTAMENTO DE TECNOLOGÍA DE YELLOWPEPPER. DSPACE.
3. Castaño María, G. C. (2015). DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRESEN EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA FUNDACIÓN NEUMOLÓGICA COLOMBIANA. Los Libertadores.
4. Cook, J., & Brockport, S. (2015). A Six-Stage Business Continuity and Disaster Recovery Planning Cycle. SAM Advanced Management Journal, 23-68.
5. El-Khouri Vidarte, N. (2016). Adaptación e implementación de un sistema autónomo de bajo coste de monitorización de calidad del agua en tiempo real.
6. Española, R. A. (01 de Octubre de 2019). Real Academia Española. Obtenido de Real Academia Española: https://dle.rae.es/riesgo?m=
7. Graiman. (2018). Graiman. Obtenido de Graiman: https://www.graiman.com/quienes-somos/

8. INEN, I. e. (2016). PROTECCION Y SEGURIDAD DE LA CIUDADANIA ─ SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (SGCN) ─ REQUISITOS (ISO 22301:2012, IDT). NTE INEN-ISO 22301, 8.
9. ISACA. (2019). COBIT-2019-Framework-Governance-and-Management-Objectives.
10. ISACA. (2019). Introducción y metodología.
11. Públicas, M. d. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: ENS.
12. S.A. Torabi, H. R. (2014). Relaciones de BIA con otros elementos de BMCS. Safety science, 15.
13. Snedaker, S., & Rima, C. (2014). Business continuity and disaster recovery planning for IT professionals.
14. Torabi, S. A., Soufi, H. R., & Sahebjamnia, N. (2014). A new framework for business impact analysis in business continuity management (with a case study). Contents lists available at ScienceDirect Safety Science.

References

1. Angel, S. (2015). Continuity management model of technological infrastructure for the operation of IT services in financial companies based on ISO 22301 and ISO 27001 standards. Application to a case study. Digital Repository University of the Americas.
2. Angela, S. (2016). DEVELOPMENT OF A BUSINESS CONTINUITY PLAN FOR THE DEPARTMENT OF TECHNOLOGY OF YELLOWPEPPER. DSPACE
3. Castaño María, G. C. (2015). DESIGN OF A RECOVERY PLAN FOR DISASTERS THE AREA OF INFORMATION TECHNOLOGIES FOR THE COLOMBIAN PNEUMOLOGICAL FOUNDATION. The liberators.
4. Cook, J., & Brockport, S. (2015). A Six-Stage Business Continuity and Disaster Recovery Planning Cycle. SAM Advanced Management Journal, 23-68.
5. El-Khouri Vidarte, N. (2016). Adaptation and implementation of a low cost autonomous system for monitoring water quality in real time.
6. Española, R. A. (October 1, 2019). Royal Spanish Academy. Obtained from the Royal Spanish Academy: https://dle.rae.es/riesgo?m=
7. Graiman. (2018). Graiman Obtained from Graiman: https://www.graiman.com/who- we are /

8. INEN, I. e. (2016). PROTECTION AND SECURITY OF CITIZENSHIP ─ BUSINESS CONTINUITY MANAGEMENT SYSTEM (SGCN) ─ REQUIREMENTS (ISO 22301: 2012, IDT). NTE INEN-ISO 22301, 8.
9. ISACA. (2019). COBIT-2019-Framework-Governance-and-Management-Objectives.
10. ISACA. (2019). Introduction and methodology.
11. Public, M. d. (2012). Methodology of Analysis and Risk Management of Information Systems. Madrid: ENS.
12. S.A. Torabi, H. R. (2014). BIA relations with other BMCS elements. Safety science, 15.
13. Snedaker, S., & Rima, C. (2014). Business continuity and disaster recovery planning for IT professionals.
14. Torabi, S. A., Soufi, H. R., & Sahebjamnia, N. (2014). A new framework for business impact analysis in business continuity management (with a case study). Contents lists available at ScienceDirect Safety Science.

Referências

1. Angel, S. (2015). Modelo de gerenciamento de continuidade de infraestrutura de tecnologia para operação de serviços de TI em empresas financeiras com base nas normas ISO 22301 e ISO 27001. Aplicação a um estudo de caso. Repositório Digital da Universidade das Américas.
2. Angela, S. (2016). DESENVOLVIMENTO DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS PARA O DEPARTAMENTO DE TECNOLOGIA DE AMARELO. DSPACE
3. Castaño María, G. C. (2015). PROJETO DE UM PLANO DE RECUPERAÇÃO PARA DESASTRES A ÁREA DE TECNOLOGIAS DA INFORMAÇÃO PARA A FUNDAÇÃO PNEUMOLÓGICA COLOMBIANA. Os Libertadores
4. Cook, J. & Brockport, S. (2015). Um ciclo de planejamento de continuidade de negócios e recuperação de desastres em seis estágios. Diário de Gerenciamento Avançado do SAM, 23-68.
5. El-Khouri Vidarte, N. (2016). Adaptação e implementação de um sistema autônomo de baixo custo para monitoramento da qualidade da água em tempo real.
6. Española, R. A. (1 de outubro de 2019). Real academia espanhola. Obtido na Royal Spanish Academy: https://dle.rae.es/riesgo?m=

7. Graiman. (2018). Graiman Obtido em Graiman: https://www.graiman.com/who- we are /
8. INEN, I. e. (2016). PROTEÇÃO E SEGURANÇA DA CIDADANIA - SISTEMA DE GERENCIAMENTO DE CONTINUIDADE DOS NEGÓCIOS (SGCN) - REQUISITOS (ISO 22301: 2012, IDT). NTE INEN-ISO 22301, 8.
9. ISACA. (2019). Objetivos do COBIT-2019-Framework-Governance-and-Management.
10. ISACA. (2019). Introdução e metodologia.
11. Público, M. d. (2012). Metodologia de Análise e Gerenciamento de Riscos de Sistemas de Informação. Madri: ENS.
12. S.A. Torabi, H.R. (2014). Relações da BIA com outros elementos do BMCS. Ciência da segurança, 15.
13. Snedaker, S., & Rima, C. (2014). Planejamento de continuidade de negócios e recuperação de desastres para profissionais de TI.
14. Torabi, S. A., Soufi, H. R., & Sahebjamnia, N. (2014). Uma nova estrutura para análise de impacto nos negócios no gerenciamento da continuidade dos negócios (com um estudo de caso). Listas de conteúdo disponíveis na ScienceDirect Safety Science.