

Plan de Recuperación ante Desastres para la reactivación económica del sector Productivo

Disaster Recovery Plan for the economic reactivation of the Productive sector

Luis Ignacio Delgado Alvarez, MSc.⁽¹⁾

John José Chamba Mera, MSc.⁽²⁾

Johnny William Santana Sornoza, MSc.⁽³⁾

(1), (3) Universidad Laica Eloy Alfaro de Manabí, Campus Pedernales, Ecuador.

(2) Delegación Provincial Manabí. Contraloría General del Estado. Ecuador.

Contactos: luisi.delgado@uleam.edu.ec; luis.delgado0113@gmail.com;

Receptado: 25/02/2018

Aceptado: 16/04/2018

Resumen

El **problema** de investigación surgió a partir del Terremoto suscitado el 16 de Abril de 2016 evidenciando el bajo nivel de conocimiento de las personas en estos eventos, su **objetivo** fue demostrar el nivel preparativo de los empleados de una empresa ante los desastres naturales, demostrados en los hallazgos de auditoria. Se tomó como referencia el personal de la Empresa AMCO, una empresa dedicada a la comercialización de combustible, radicada en la Ciudad de Manta. Como **metodología** se usó la recopilación de información, suministrada por la empresa por medio de entrevistas con preguntas precisas usadas en Estándares de Seguridad Informática como son las ISO 22301 y 27001, para determinar la situación actual de sus medidas de seguridad en el área de sistemas, comprobándose ciertas fallas que conllevaron al mejoramiento y cumplimiento de estándares mínimos de seguridad. El **resultado** del estudio fue el *Plan de Recuperación ante Desastres* que describe los riesgos que pueden sufrir los empleados, **concluyendo** que las acciones correctivas a tomarse en el caso de ocurrir el incidente, minimizarán los daños en los desastres y optimizarán la restauración oportuna de los servicios.

Palabras Claves: Desastres, Seguridad Informática, DRP, BCP, Backup.

Abstract

The problem that arises from the Earthquake that arose on April 16, 2016 evidencing the low level of knowledge of the people in these events, its objective was to demonstrate the preparatory level of the employees of a company faced with natural disasters, demonstrated in the audit findings. The personnel of the Company AMCO, a company dedicated to the commercialization of fuel, based in the City of Manta, was taken as a reference. As a methodology, information gathering was used, provided by the company through interviews with precise questions used in Information Security Standards such as ISO 22301 and 27001, to determine the current status of their security measures in the systems area, checking certain failures that led to the improvement and compliance with minimum safety standards. The result of the study was the Disaster Recovery Plan that describes the risks that employees may suffer, concluding that the corrective actions to be taken in the event of the incident, will minimize damage in disasters and optimize the timely restoration of services. .

Key Words: Disasters, Computer Security, DRP, BCP, Backup.

Introducción

Los Desastres son hechos que suceden de forma repentina o prevista que alteran la normalidad de actividades en la sociedad, que pueden ser causados por la naturaleza o por actividades humanas, dejando consecuencias en esta sociedad, como son las pérdidas económicas, materiales, humanas y ambientales (IFRC, 2018).

El Plan de Recuperación ante Desastres (siglas DRP del Inglés Disaster Recovery Plan) es un proceso detallado y respaldado en documentos que servirá para la recuperación y protección de los recursos tecnológicos de una empresa. Incluido dentro del BCP (Plan de Continuidad del Negocio), que es un conjunto de planes que ayudará para continuidad de los negocios en la empresa (Sanchez, 2013).

El DRP aborda en tres fases su aplicación: antes del desastre, durante el desastre y después del desastre. De esta forma una empresa se asegura la continuidad del negocio abarcando los escenarios principales que hayan pasado en empresas similares de la región. “Antes del Desastres (Prevención) donde pretende asegurar los sistemas importantes y críticos, protegiendo sus datos y capacitar al personal encargado de recuperarlos en caso de una interrupción. Haciendo que esta recuperación sea eficaz”, (Loza, 2013).

Durante el desastre (Continuidad) cuyo fin sería mantener y continuar esos procesos recuperados para que la empresa funcione con sus operaciones, comprende en esta fase el mantenimiento de los sistemas y sus recursos, como los traslados a sitios secundarios durante el desastre, (Federacion Internacional de sociedades de la Cruz Roja, 2016). Después del desastre (Recuperación) con el objetivo de restaurar todos los sistemas y recursos al estado normal y en correcto funcionamiento, regresando a su sitio original. (Mifsut, 2012).

El propósito del DRP es mantener funcionales los sistemas informáticos e incorporar nuevas soluciones para la optimización de los procesos de la empresa. Este plan está dirigido al área de tecnología, que tiene sus bases en el estándar británico 25999 y en las normas ISO 27001 y 22301, que nos van a ayudar a elaborar el plan de recuperación ante desastres para poder contar con una serie de procedimientos a seguir direccionados a la mitigación del suceso. Luego de seguir una evaluación de cual norma utilizar para realizar el DRP, se escoge la ISO 22301 por ser la más adecuada y utilizada al nivel mundial en implementación de Planes de Continuidad de Negocios (BCP) (Rodríguez, 2014).

Para el cumplimiento de la norma se deben de recopilar información que establece la norma (ISO 22301, 2012), con lineamientos específicos basados en un ciclo repetitivo y continuo que lo mantiene actualizado llamado ciclo de Deming PDCA; el cual se divide en cuatro etapas para definir los procesos críticos de tecnología que debe de soportar las operaciones de un negocio en sus actividades habituales cuando se presente una crisis.

El Ciclo de Deming PDCA viene del Significado de sus siglas en Inglés PLAN, DO, CHECK, ACT. Cada Sigla es una fase o etapa que describe un número de documentos que se deben emplear con el fin de soportar la operación de todos los procesos de tecnología que se requieran dentro de las actividades diarias, (Rojo, 2013).

Se detalla a su vez la importancia e introducción de la fase de planificación, la misma que tiene como objetivos y procesos necesarios el alcanzar los resultados requeridos por la organización, recopilando datos que ayuden en la comprensión de estos procesos, (ICETEX, 2013). Los documentos necesarios son el procedimiento para identificación de requisitos, la lista de requisitos legales, normativos y contractuales, tener clara la política para la recuperación ante desastres que va en respaldo del plan de capacitación y concienciación.

Consecuentemente en la fase de realización (DO), para la implementación de nuevos procesos, “es recomendable realizarlos a través de pruebas piloto para ir verificando su correcto

funcionamiento antes de su aplicación final, en donde se debe utilizar los documentos para evidenciar la metodología para el análisis del impacto en el negocio, cuestionario sobre el análisis del impacto en el negocio, estrategia de recuperación ante desastres, lista de actividades, prioridades de recuperación para las actividades, establecer los objetivos de tiempo de recuperación para las actividades y preparación para la continuidad de los servicios de T.I., desarrollando estrategias de recuperación de actividades” (SGC-MAP, 2014).

Es menester establecer dentro de la fase de realización el plan de recuperación ante desastres, de respuesta a los incidentes, mantener el registro de incidentes para ubicaciones para la continuidad de las operaciones con el debido plan de transporte y recuperación de actividad.

Así mismo se contempla la fase de verificación (CHECK), “durante un tiempo de prueba establecido, se verifica el correcto funcionamiento de la mejora implantada. Si los resultados no son los esperados, se realizan cambios para conseguir los objetivos deseados” (Arias, 2014).

Siendo los documentos para la ejecución de esta etapa el plan de prueba, mantenimiento y revisión del DRP, el informe de pruebas y verificación, creación un plan de mantenimiento y revisión del DRP, desarrollar el formulario de revisión postincidente para el procedimiento para auditoría interna dentro del programa anual, establecido mediante minutas de revisión por parte de la dirección.

En la fase de ajuste en la aplicación de mejoras cuando se detectan errores durante la ejecución de una iteración del modelo “se deben realizar el procedimiento para medidas correctivas y el formulario para medidas correctivas, donde se procede agrupar los criterios en una tabla para posterior calificar basándonos con un juicio personal una vez analizados los estándares declarados” (Drake, 2013).

Objetivos específicos

- Definir y comprender los servicios, procesos y recursos críticos que estén inmersos en la unidad de T.I. de la corporación AMCO,
- Analizar estándares de continuidad acordes al negocio, tendencias actuales y realidad del entorno en la unidad de T.I. donde opera la corporación AMCO.
- Ejecutar pruebas piloto para el plan de recuperación ante desastres.

Materiales y Métodos

La investigación es de tipo cualitativo descriptivo y de corte transversal, como métodos teóricos se utilizó el método deductivo, como métodos empíricos se utilizaron los registros que fueron adquiridos a partir de la recopilación de auditorías externas hechas en la empresa; De los incidentes ocurridos como fueron la propagación de malware, caídas del servicio por hardware obsoleto y por proveedor de servicio de internet desde el 2014 al 2016.

Adicionalmente se usó listas de comprobación que demanda la norma ISO 22301 para su cumplimiento de la continuidad de los servicios; también se realizaron encuestas que fueron hechas al personal en el área de TI de la Empresa y de las entrevistas dirigidas al Gerente de TI y Gerente Financiero.

Los materiales utilizados fueron los equipos informáticos del área de TI. Sólo se incluyó sólo el área de TI, porque el Plan de Recuperación ante Desastres se centra en los recursos del área de Tecnología.

Resultados

Los resultados estructurados dentro del esquema de pruebas y su análisis del DRP, donde se conoce que en base al plan de recuperación se procederán a hacer pruebas o simulacros tomando como estándar la (ISO 22301, 2012) que permite medir la eficiencia y aplicación ante estos eventos adversos, para lo cual se aplicaron los siguientes procedimientos:

- a) Control de documentos y registros
- b) Plan del Proyecto
- c) Procedimiento para identificación de requisitos
- d) Política para la recuperación ante desastres
- e) Metodología para el análisis del impacto en el negocio
- f) Estrategia de recuperación ante desastres
- g) Plan de recuperación ante desastres
- h) Plan de Pruebas, mantenimiento y revisión del DRP.
- i) Plan de capacitación y concienciación
- j) Procedimiento para auditoría interna
- k) Procedimiento para medidas correctivas

Al efectuar el plan de recuperación ante desastres de la unidad de T.I. de AMCO, se evidenció algunas dificultades en los procesos y recursos críticos, como la poca disponibilidad de tiempo

de los integrantes de la Unidad de T.I. y de otros departamentos en sus actividades diarias, así mismo la carencia de capacitaciones de los que conforman la unidad de T.I.

Así mismo se pudo conocer que los tiempos prolongados durante la implementación del DRP para la Unidad de T.I. de AMCO, presentaron inconvenientes en la realización de pruebas piloto en tiempo real, como las carencias presentadas en la definición de la criticidad de los servicios, debido a la poca difusión del plan dentro de la Corporación; de la misma forma los eventos externos inesperados que atrasaron la implementación del plan de recuperación.

La aplicación del DRP en la corporación AMCO, proyectaron buenos resultados. Los escenarios aplicados garantizan una recuperación de los servicios de forma satisfactoria, que va de la mano con los objetivos de la corporación según el correcto uso de la documentación de la corporación con la que se trabajó, misma que presenta su situación actual omitiendo datos considerados sensibles para AMCO.

Se toma en cuenta los sistemas de respaldo utilizados por AMCO, en base a la ejecución del plan de recuperación ante desastres que permite disminuir los riesgos en la pérdida de información, también durante la realización del análisis de impacto se evaluaron los diferentes servicios distribuidos por su tipo (telecomunicaciones y sistemas y aplicativos).

Cada rol dentro del DRP tiene asignado su respectivo backup en cuanto a los temas de confidencialidad, se omiten algunos sistemas y aplicativos y demás recursos utilizados por la corporación AMCO, a más de ello se identificaron los conocimientos adquiridos gracias a la investigación de propagación de un malware tipo troyano.

Los integrantes de la unidad de T.I. dieron respuesta en lapsos establecidos en las caídas en el servicio de telecomunicaciones por hardware con averías, teniendo en cuenta los resultados obtenidos en la aplicación del modelo se corrobora su utilidad para la corporación AMCO, para reforzar la aplicación del modelo, se recomendó su aplicación en escenarios más complejos. A continuación se detalla el resultado del cuestionario para el análisis de impacto para negocios de la empresa enfocado en el servicio de telecomunicaciones que es el servicio principal para que los demás sistemas funciones luego de una interrupción:

1. Información general sobre la actividad						
Nombre de la organización:	AMCO	Nombre de la persona responsable:	Asistente de soporte de hardware			
Nombre de la actividad:	Minimizar el incidente, estableciendo acciones preventivas y correctivas en los dispositivos de telecomunicaciones para asegurar su disponibilidad.	Correo electrónico:	arojas@amco.com.ec			
Domicilio:	Manta, Av. 113 y Calle 319	Fecha:	14 de enero de 2017			
2. Descripción de la actividad						
Breve descripción de la actividad:	Tareas clave y obligaciones legales y/o contractuales: Plazos de ejecución:					
Garantizar la disponibilidad necesaria de los servicios brindados por los dispositivos de telecomunicaciones y los que dependen de ellos, para que puedan operar los sistemas utilizados habitualmente en las actividades principales de AMCO en su matriz y las sucursales	Revisar el funcionamiento de los dispositivos de telecomunicaciones	30 minutos				
	Monitorear Constantemente los dispositivos de telecomunicaciones	10 minutos				
	Revisar notificaciones de incidentes y conexiones de los dispositivos de telecomunicaciones.	10 minutos				
	Reactivación del servicio reportado en el incidente.	15 minutos				
	Mantenimiento y limpieza física de los dispositivos de telecomunicaciones	30 minutos				
	Comprobar un adecuado Ambiente de operación de los dispositivos de telecomunicaciones	10 minutos				
3. Impacto general del incidente disruptivo (1 – consecuencia insignificante; 2 – consecuencia aceptable; 3 – consecuencia mayor; 4 – consecuencia catastrófica)						
	Descripción (si fuera necesario)	2 horas	4 horas	24 horas	48 horas	1 semana
Pérdida de la reputación de la organización en el mercado:	Posicionamiento en el mercado frente a competencias	1	2	3	3	4
Reacciones de los clientes:	Opinión de clientes cuando cesan actividades	1	2	3	3	4
Impacto sobre otras actividades de la organización:	Otras actividades afectadas por la paralización de actividades	1	2	3	3	4
Consecuencias sobre la salud y seguridad del personal; consecuencias sobre el medioambiente:	Como es afectada la salud de los empleados cuando ocurre la paralización de los servicios	1	1	1	1	1
Qué tan difícil será ponerse al día con el trabajo atrasado:	Dificultades para ponerse al día posterior a la suspensión	2	2	3	4	4
4. Impacto financiero del incidente disruptivo: ¿Cuál sería la pérdida financiera producida por el incidente disruptivo? (en dólares)						
	Descripción (si fuera necesario)	2 horas	4 horas	24 horas	48 horas	1 semana
Consecuencias legales:	Pérdidas ocasionadas y gastos generados por incumplimiento					
Consecuencias contractuales:	Pérdidas ocasionadas por pago de multas					
Pérdida de ingresos de potenciales clientes:	Pérdida por ventas no realizadas a clientes nuevos					
Pérdida de ingresos de clientes actuales:	Pérdida por ventas no realizadas a clientes habituales					
Gastos adicionales (reparaciones, mantenimiento, etc.)	Gastos por los mantenimientos, reparaciones, movilizaciones, etc	0	0	500	1'500	8'000
5. Comentarios / otra información importante:						
En caso de ocurrir una interrupción en los SERVICIOS DE TELECOMUNICACIONES, este incidente suspendería las actividades principales en AMCO, lo que implica pérdidas económicas considerables para la empresa.						
6. Conclusiones (a completar por el Coordinador del DRP)						
aceptable):		4 horas				

7. Cantidad de trabajo	
Período(s) con mayor cantidad de trabajo:	Los meses de Abril, Mayo y Noviembre
Cantidad de trabajo realizada durante períodos con mayor cantidad de trabajo:	7 incidentes resueltos
Cantidad mínima aceptable de trabajo para la actividad crítica inmediatamente después del desastre:	2 incidentes resueltos
Período a partir del cual se debe retomar la cantidad de trabajo o nivel de funcionamiento normal:	24 horas

8. Recursos necesarios para la recuperación										
Nombre del recurso	Información específica	Cantidad	Punto único de falla	Tiempo a partir del cual es necesario el recurso						
				inmediatamente	1 hora	4 horas	24 horas	2 días	1 semana	otro (especificar)
Personas:										
Jefe de Tecnología	Liderazgo, Configuración de Routers, Switch, Firewall, Antispam, Cableado Estructurado	1	X	X						
Asistente técnico de hardware	Switch, Firewall, Antispam, Cableado Estructurado, Monitoreo Redes	1			X					

Aplicaciones / bases de datos:										
Sistema Operativo de UTM	Software para actualización del UTM	1		X						
Sistema Operativo de Switches	Firmware de actualización para los Switches	5		X						
Sistema Operativo de Central Telefonica IP	Software para actualización de la Central IP	1		X						
Sistema Operativo para Emails	Software de instalación Linux y Zimbra	1		X						
Datos almacenados en formato electrónico (no incluidos en aplicaciones / bases de datos):										
Respaldo de configuraciones de los equipos de telecomunicaciones	Datos almacenados en el Storage General	3			X					
Arquitectura de la red	Datos almacenados en el Storage General	1		X						
Manuales digitales de equipos	Disponibles en Pagina del Fabricante	8		X						
Respaldo de base de datos de los equipos	Datos almacenados en el Storage General	2			X					
Datos almacenados en papel:										
Arquitectura de la red	Archivador del Jefe de TI	1								Solamente cuando el caso amerite
Manuales de configuración	Archivador del Jefe de TI	1								Solamente cuando el caso amerite
Contactos	Archivador del Jefe de TI	1								Solamente cuando el caso amerite

Equipos de TI y comunicaciones:										
Equipos de Escritorio										
Portátiles										
Servidores	Servidor Zimbra Virtualizado Servidor Denwa Pro / Mini	4	X	X						
Switches de AMCO (Cantidad por cada fila un modelo)	3Com Baseline 2924	2	X	X						
	HP ProCurve 2910a1-24G	1	X	X						
	3Com Baseline 2916	1	X	X						
	3Com Baseline 2928	2	X	X						
	HP V1910-24G	8	X	X						
	HP V1910-48G	1	X	X						
Firewalls de AMCO (Cantidad por cada fila un modelo)	Sophos UTM 220	1	X	X						
Routers de AMCO (Cantidad por cada fila un modelo)	Sophos UTM 220 Switch Procurve	2	X	X						
Impresoras de AMCO (Cantidad por cada fila un modelo)										
Telefonos de AMCO (Cantidad por cada fila un modelo)	Denwa IP DW-310P	78			X					
	Denwa IP DW-610P	4			X					
	Denwa IP DW-800	7			X					
Telefonos celulares de AMCO (Cantidad por cada fila un modelo)	Samsung Galaxys desde J5 a S5									

Canales de comunicación:										
Líneas Fijas	Telefonia IP	4			X					
Líneas Celulares	Telefonia Movistar Jefatura TI	1		X						
Acceso a Internet	Telefonia Movistar (Internet 12 Mbps) Telconet (Internet 8Mbps y Canales de Datos Sucursales 2 Mbps)	2								Se mantiene redundancia de servicios
Correo electrónico	Cuentas de correos activas	4		X						
Otros equipos:										
TV										
Radio										
Instalaciones e infraestructura:										
Puntos de Red para los computadores	Puntos de Voz y Datos Cat. 6A	8		X						
Backbone de servidores	Puntos de Voz y Datos Cat. 6A de Matriz y Sucursales	285		X						
Muebles de oficina		4			X					
Capital de trabajo necesario:										
Capital para material necesario no existentes	Habilitación Red Interna, Internet y Tuneles de Datos	47825		X						
Servicios externos:										
Servicio Eléctrico		3		X						
Agua Potable		3		X						
Alquiler Oficinas										

9. Dependencia de terceros (quién es necesario para la recuperación de esta actividad)						
Dependencia de otras actividades de la organización:	Departamento de Compras de la Empresa	Procedimiento de Compras y Selección de Proveedores				3
	Departamento Financiero de la Empresa					3
Dependencia de socios:						
Dependencia de proveedores:	Telconet	Contratos de Servicios de Internet				3
	Telefónica Movistar	Contratos de Servicios de Internet				3
	CNEL (Empresa Eléctrica)	Contratos de Servicios de Suministro Eléctrico				2
	CNT	Contratos de Servicios Telefónico				2
	Empresa de Agua Potable	Contratos de Servicios de Agua Potable				2
	ALLSERVICES	Contratos de Servicios de Redes y Mantenimiento				3
10. Pérdida máxima de datos: cantidad de datos que se pueden perder (1 - consecuencia insignificante; 2 - consecuencia aceptable; 3 - consecuencia mayor; 4 - consecuencia catastrófica)						
	1 hora	4 horas	24 horas	48 horas	1 semana	¿Con qué frecuencia?
Aplicaciones / bases de datos:						
Sistema Operativo de UTM	2	3	3	4	4	Solamente cuando hay cambios
Sistema Operativo de Switchs	1	2	3	3	4	
Sistema Operativo de Central Telefonica IP	1	2	3	3	4	Solamente cuando hay cambios
Sistema Operativo para Emails	1	2	3	3	4	Solamente cuando hay cambios
Datos almacenados en formato electrónico:						
Respaldo de configuraciones de los equipos de telecomunicaciones	1	1	2	2	3	Respaldo diario
Arquitectura de la red	1	1	2	2	3	Solamente cuando hay cambios
Manuales digitales de equipos	1	1	2	2	3	Solamente cuando hay cambios
Respaldo de base de datos de los equipos	1	1	2	2	3	Respaldo diario
Datos almacenados en papel:						
Arquitectura de la red	1	1	2	2	3	
Manuales de configuración	1	1	2	2	3	
Contactos	1	1	2	2	3	
11. Alternativas en el caso de un desastre						
¿Pueden otras actividades continuar con el funcionamiento de esta actividad? En caso afirmativo, ¿cuáles?	Dependiendo del tipo y nivel del desastre se podrían activar otros medios de comunicación de datos como los celulares y correos personales.					
¿Es posible realizar algunas actividades en forma manual, sin equipos de TI ni de otro tipo?	NINGUNA POSIBLE					
12. Experiencias anteriores						
¿Con qué frecuencia se han producido incidentes disruptivos en el negocio hasta ahora? ¿Cuánto tiempo duraron?	Generalmente ha habido dos o tres eventos al año considerando también las comunicaciones con las sucursales. Desde 30 minutos hasta 2 horas.					
¿Cómo se manejaron esas situaciones?	Cuando la solución ha dependido de nuestros propios recursos ha sido resuelto inmediatamente. Cuando ha involucrado recursos externos como proveedores hemos tenido que esperar que el problema sea resuelto por ellos.					
13. Comentarios / otra información importante:						
El Servicio de telecomunicaciones de la Unidad de TI, es primordial para el funcionamiento de todas las actividades de AMCO						

Tabla 1. Cuestionario sobre el análisis del impacto en el negocio.

Fuente: Departamento de Tecnología de AMCO.

Partiendo de los resultados obtenidos en las pruebas, se iniciaron mediante la aplicación del DRP se evidenció la necesidad de adquisición de licencias corporativas de antivirus, el etiquetado de cables de red para su posterior identificación, la adquisición de hardware de respaldo para las telecomunicaciones para efectuar y coordinar capacitaciones continuas y en horarios flexibles para todos los integrantes involucrados en el plan.

Discusión

Se conoce que dentro del plan efectuando en las pruebas de mantenimiento y revisión del DRP, encontrando que se cumplan parámetros para reforzar el sector productivo, es necesario el contar con un plan de recuperación de desastres que permita estar preparados para incidentes que puedan incurrir en una afectación directa al funcionamiento de una organización en la pérdida de datos, debiendo adoptar planes que sirvan como herramienta indispensable, permitiendo su estabilidad en el mercado, donde se exponen las siguientes investigaciones.

Se menciona en un estudio realizado por la empresa VP de VMware Latinoamérica muestra que para comprender los servicios, procesos y recursos críticos que estén inmersos en la unidad de T.I., muestra que es importante la recuperación de desastres según la interrupción del servicio o la pérdida de información, la misma que tiene un impacto crítico en las finanzas; Por lo tanto, el DRP en la virtualización obtenida representa un avance considerable según la encuesta de Acronis, las razones principales por las que se adopta un mejoramiento en los servicios, procesos y recursos críticos, enfocados a la eficiencia mejorada (24%); flexibilidad y velocidad de implementación (20%) y reducción de costos (18%), (Pérez, 2013).

A consecuencia se realizó un informe de pruebas, verificación con el fin de informar sobre los objetivos que se hayan alcanzado o no en la prueba aplicada mediante el plan de recuperación ante desastres de la unidad de T.I. de AMCO, se evidenció que dentro de los servicios, procesos y recursos críticos que están inmersos en la unidad de T.I. de la corporación AMCO, existen algunas dificultades en los procesos y recursos críticos, como la poca disponibilidad de tiempo de los integrantes de la Unidad de T.I. y de otros departamentos en sus actividades diarias, así mismo la carencia de capacitaciones de los que conforman la unidad de T.I.

Reconociendo el objetivo en cuanto a definir y comprender los servicios, procesos y recursos críticos que estén inmersos en la unidad de T.I. la empresa VP de VMware Latinoamérica se reconoce que al implementar el plan en la unidad de T.I. en la aplicación del DRP se encuentran listas, inventarios, copias de seguridad de software y datos, cualquier otra lista importante de materiales, donde mantiene un mejoramiento en los servicios, enfocados a la eficiencia mejorada; procesos debido a la flexibilidad y velocidad de implementación y recursos críticos en la reducción de costos, como también en la unidad de T.I. de AMCO, es menester que dentro de los servicios, procesos y recursos críticos se encontraron algunas dificultades en los procesos

y recursos críticos, como la poca disponibilidad de tiempo de los integrantes de la Unidad de T.I. y de otros departamentos en sus actividades diarias.

En un estudio efectuado en base a los estándares de continuidad acordes al negocio, tendencias actuales y realidad del entorno donde opera la compañía System Integration en Alestra, se conoce que “de acuerdo con datos obtenidos se especula una pérdida de registros automatizados por un desastre, solo el 6% sobrevive a largo plazo, 51% cierra en menos de un año y 43% nunca vuelve a abrir, contando con una aplicación DRP, elemento que se considera fundamental en la estrategia para mejorar los estándares de continuidad acordes a la compañía” (Alestra, 2014).

De la misma forma aplicando un formulario de revisión postincidente que se ejecutara al momento de que suceda algún incidente fuera de los escenarios planteados inicialmente para que pueda ser incluido en las acciones correctivas del DRP. AMCO, se pudo conocer que los tiempos prolongados durante la implementación del DRP para la Unidad de T.I. de AMCO, en cuanto a los estándares de continuidad acordes al negocio, tendencias actuales y realidad del entorno donde opera la compañía presentaron inconvenientes en la realización de pruebas piloto en tiempo real, como las carencias presentadas en la definición de la criticidad de los servicios, debido a la poca difusión del plan dentro de la Corporación; de la misma forma los eventos externos inesperados que atrasaron la implementación del plan de recuperación.

Como muestra Alestra en base a los estándares de continuidad acordes al negocio, tendencias actuales y realidad de la compañía System Integration en Alestra, evidencia que existe una pérdida de registros automatizados según las tendencias actuales por desastres, donde solo un 6% sobrevive a largo plazo viendo la necesidad de establecer estrategias para mejorar los estándares de continuidad con el fin de asegurar el capital para otorgar los mejores rendimientos, contando con un proveedor especializado y experimentado que garantice los recursos apropiados, procesos y herramientas para una contingencia es lo más recomendable; En forma continua se conoce que AMCO, presenta inconvenientes en la realización de pruebas piloto en tiempo real, como las carencias presentadas en la definición de la criticidad de los servicios, debido a la poca difusión del plan dentro de la Corporación; de la misma forma los eventos externos inesperados que atrasaron la implementación del plan de recuperación.

En un artículo realizado por José Loor, considera que dentro de las pruebas pilotos aplicadas en el plan de recuperación ante desastres se desarrolló en base al DRP simulacros o pruebas

pilotos a la unidad de servicios informáticos, con tres escenarios seleccionados para medir el grado de eficacia y aplicabilidad, seleccionados de forma discrecional, siguiendo el esquema que manda la norma ISO 22301:2012, las pruebas pilotos se realizaron con éxito, demostrando el beneficio de contar con procedimientos ordenados en un plan de respuesta a incidentes, donde cada persona sabe cómo actuar y los recursos de los que dispone, (Loor, 2015).

A su vez en la Corporación AMCO en las pruebas piloto del plan de recuperación ante desastres, es necesario preparar a todo el personal que cumple una función en el DRP y debe cumplirla eficazmente, donde se describen las actividades que tengan relación con la auditoría, mismas pruebas que permitieron disminuir los riesgos en la pérdida de información, también durante la realización del análisis de impacto se evaluaron los diferentes servicios distribuidos por su tipo (telecomunicaciones y sistemas y aplicativos) datos que fueron obtenidos mediante el cuestionario sobre el análisis del impacto en el negocio – Servicios de Telecomunicaciones.

Conclusiones

- En la definición y comprensión en los servicios procesos y recursos críticos aplicando un DRP en la unidad de T.I. ayuda estrechamente al mejoramiento en los servicios, enfocados a la eficiencia mejorada; procesos debido a la flexibilidad y velocidad de implementación y recursos críticos en la reducción de costos, de manera que se identifican riesgos así como sus impactos, debido a que serán considerados para el análisis y posterior aplicación de medidas correctivas.
- De entre los diferentes estándares existentes en la actualidad referente a la continuidad de las operaciones y a la recuperación ante desastres, el estándar elegido representa la mejor elección para la unidad de tecnología de la corporación AMCO, corroborándose lo anterior con los diferentes escenarios planteados en los cuales se pudo evidenciar su practicidad y eficacia.
- En la aplicación del plan de las pruebas piloto se pudo conocer que la misma ayuda y colaboración de la unidad de T.I. además de sus esquemas de disponibilidad y respaldos de información, el desarrollo del presente Plan de Recuperación ante desastres es exitoso, ya que ayudará significativamente para su aplicación, conocimiento y comprensión del estándar elegido.

Referencias.

- Alestra, I. F. (Octubre de 2014). *Consejos para establecer un Plan de Recuperación de Desastres (DRP)*. Obtenido de <http://searchdatacenter.techtarget.com/es/opinion/Consejos-para-establecer-un-Plan-de-Recuperacion-de-Desastres-DRP>
- Arias, C. A. (2014). *La Gestión De Los Procesos*. Obtenido de <http://webs.ucm.es/centros/cont/descargas/documento10142.pdf>
- Drake, J. M. (2013). *Programación orientada a objetos: Lenguajes, Metodologías y Herramientas Master de Computación*. Obtenido de https://www.ctr.unican.es/asignaturas/MC_OO/Doc/OO_08_I2_Proceso.pdf
- Federacion Internacional de sociedades de la Cruz Roja. (5 de Abril de 2016). *Federacion Internacional de sociedades de la Cruz Roja*. Obtenido de Federacion Internacional de sociedades de la Cruz Roja: Recuperado de: <http://www.ifrc.org/es/introduccion/disaster-management/sobre-desastres/que-es-un-desastre/>
- ICETEX. (30 de Mayo de 2013). *MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DE NEGOCIOS*. Obtenido de https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf
- IFRC. (24 de Febrero de 2018). *Federacion Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja*. Obtenido de <http://www.ifrc.org/es/introduccion/disaster-management/sobre-desastres/que-es-un-desastre/>
- ISO 22301. (2012). *Seguridad de la Sociedad: Sistemas de Continuidad del Negocio*. ISO.
- Loor, J. (2015). *Desarrollo de un plan de recuperación de desastres para la unidad de tecnología de la empresa pública municipal de agua potable y alcantarillado de Portoviejo*. Sangolquí, Ecuador: Universidad de las Fuerzas Armadas.
- Loza, P. (s.f. de s.f. de 2013). *Desastres naturales inesperados*. Obtenido de <http://www.iadb.org/es/acerca-del-bid/desastres-naturales-inesperados,6675.html>

- Mifsut, E. (26 de Marzo de 2012). *Introduccion a la Seguridad Informática*. Obtenido de <http://recursostic.educacion.es/observatorio/web/en/software/softwaregeneral/1040-introduccion-a-la-seguridad-informatica?showall=1>.
- Pérez, A. L. (Noviembre de 2013). *Pasos para un Plan de Recuperación de Desastres (DRP)*. Obtenido de <http://searchdatacenter.techtarget.com/es/cronica/Pasos-para-un-Plan-de-Recuperacion-de-Desastres-DRP>
- Rodruiguez, L. E. (s.f. de s.f. de 2014). *PLAN DE CONTINUIDAD BS 25999*. Obtenido de http://sisteseg.com/files/Microsoft_Word_-_Articulo_BS_25999_DEF1.pdf
- Rojo, A. (Junio de 2013). *El ciclo de Deming o círculo PDCA*. Obtenido de <https://www.s bqconsultores.es/el-ciclo-de-deming-o-circulo-pdca/>
- Sanchez, N. (1 de Marzo de 2013). *CELINGEST*. Obtenido de <http://blog.celingest.com/2013/03/01/recuperacion-desastres-disaster-recovery/>
- SGC-MAP. (2014). *Guía para la elaboración e implementación del plan de mejora institucional*. Obtenido de <https://map.gob.do/wp-content/uploads/2012/04/GUIA-para-la-Elaboracion-e-Implementacion-del-Plan-de-Mejora-Institucional.pdf>