DESARROLLO DEL PLAN DE CONTINGENCIA PARA SISTEMAS DE INFORMACION CON BASE EN LA NORMA NIST 800-34

Díaz Rodríguez, Diana Carolina.
Diana_75323@hotmail.com
Universidad Piloto de Colombia

Abstract— The purpose of this document is to establish the main characteristics and actions to be taken into account in the business continuity management plan guide, which today's companies can put into practice for their information systems since in the At the moment of presenting faults in the provision of the service, it provides assistance in the reestablishment of the functions as quickly as possible and in this way helps that the losses and sanctions are not devastating for the organizations.

Resumen—El presente documento, tiene como finalidad establecer las principales características y acciones a tener en cuenta en la guía del plan de gestión de la continuidad del negocio, que las empresas de hoy en día pueden poner en práctica para sus sistemas de información ya que en el momento de presentar fallas en la prestación del servicio brinde una ayuda en el restablecimiento de las funciones lo más rápido posible y de esta manera ayudar a que las pérdidas y sanciones no sean devastadoras para las organizaciones.

Índice de Términos—Gestión del plan de continuidad, gestión de riesgo, inventario de activos, Objetivos de la norma Nist 800-34, Sistemas de información.

I. INTRODUCCIÓN

Hoy en día las empresas sin importar su actividad comercial y el área en el que desempeñen sus relaciones de negocios reciben, almacenan, procesan y generan información. Dependiendo de la cantidad que manejen se hace necesario el uso de los sistemas de información y estos se han convertido en una parte fundamental en la prestación de servicios por muchas organizaciones que han entendido que para hacer más productivas la gran parte de sus procesos deben ser automatizados a través de sistemas de información, los cuales ayudan a un procesamiento mucho más rápido y obtienen los resultados necesarios en un tiempo muy corto y se pueden acceder desde cualquier dispositivo en tiempo real, para de esta forma generar agilidad a la hora de la toma de decisiones y determinaciones de las organizaciones, la disponibilidad de los datos y su fácil acceso para los interesados generan efectos muy positivos en el crecimiento de las empresas actualmente.

De acuerdo con la definición de sistema de información es un conjunto de componentes relacionados que recolectan, procesan, almacenan y distribuyen información que ayuda a la toma de decisiones en las organizaciones [1].
Los sistemas de información cumplen las siguientes funciones básicas, reciben información a lo que se conoce como entrada, realizan procesamiento, que algunas veces necesitan que sea almacenado el resultado de este y por último se obtiene la salida de información [2].

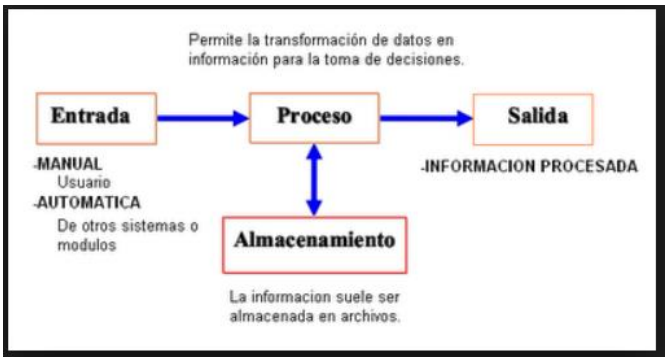

Fig. 1. Actividades básicas de un sistema de información, Obtenida de https://izamorar.com/actividades-basicas-de-un-sistema-de-informacion/

De acuerdo lo anterior el presente documento ayuda a establecer las características principales que se deben de tener en cuenta a la hora de establecer la guía para el plan de continuidad del negocio en los sistemas de información y de esta forma que los procesos que llevan a cabo las organizaciones tengan lo menos posible efectos negativos, cuando se presente un fallo y la interrupción no genere multas y pérdidas económicas que puedan afectar el funcionamiento normal de las empresas.

II. TIPOS DE SISTEMAS DE INFORMACIÓN

En el ámbito de negocios donde se desempeñan la mayoría de las organizaciones de hoy en día, la información se ha convertido en una parte fundamental para el funcionamiento de estas, por ende, se hace necesario la implementación de sistemas de información que ayudan a establecer metas y estrategias con el objetivo de ser más productivas y competitivas en el mercado actual, por tanto existen diversos sistemas de información, cuyo objetivo es ayudar a agilizar el procesamiento de los datos y tenerlos disponibles para su consulta de acuerdo a como lo necesite la organización, a continuación se relacionan los más importantes.

A. Sistema de procesamiento de transacciones (Transaction Processing System TPS)

Este proceso es el encargado de registrar las transacciones dentro y fuera de la empresa, un ejemplo de este sistema es una compra mediante tarjeta de crédito en un sitio web [3].

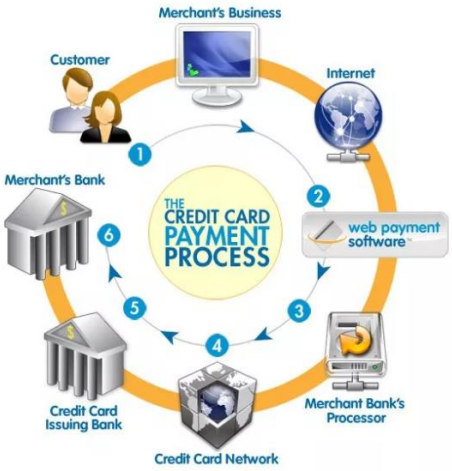

Fig. 2. Proceso de compra a través de una tarjeta crédito en un sitio web, mediante transacciones y un SI TPS, Obtenida de https://tiposdesistemasdeinformacion.wordpress.com/2015/04/09/sistema-de-procesamiento-de-transacciones-tps/

B. Sistemas de información administrativa (Management Information System MIS)

Este sistema proporciona a la compañía ayuda para organizar la información con el fin de ayudar a los líderes en la toma de decisiones, entre los principales componentes de este sistema son el software como bases de datos, aplicaciones, adicionalmente el hardware y recursos humanos necesarios para su adecuado funcionamiento, la implementación de este sistema provee más eficiencia a las organizaciones.

Fig. 3. Componentes de un MIS, Obtenida de https://www.toppr.com/guides/accountancy/application-of-computers -in-accounting/management-information-systems-and-accounting-information-system/

C. Sistemas de información contable (Accounting Information System AIS)

Este sistema proporciona ayuda a la compañía en la toma de decisiones a nivel financiero, debido a que recibe, procesa, analiza y almacena datos financieros de la organización proporcionando los informes necesarios, al igual que el MIS posee componentes de hardware, software y recursos humanos [4].

III. GESTIÓN DE RIESGOS EN SISTEMAS DE INFORMACIÓN

Antes de definir el plan de contingencia, la organización debe realizar un exhaustivo análisis y gestión del riesgo con el fin de identificar y realizar un inventario de los activos de los sistemas de información más críticos que deben reestablecer su servicio lo más pronto posible en cuanto se materialice un riesgo y de esta manera evitar que el impacto negativo sea mayor para la empresa.

La gestión del riesgo consiste en como primer punto realizar un inventario de activos y definirlos, darles una clasificación de acuerdo a su nivel de importancia para la empresa, identificar las amenazas y vulnerabilidades que los pueden poner en riesgo y de esta manera generar afectación en el funcionamiento normal de las organizaciones, para realizar una gestión adecuada de los riesgos se deben seguir los siguientes pasos.

1. Gestión de activos de información

En la gestión de los activos se deben realizar varias acciones como lo son un inventario de activos, en el cual se identifiquen todos los activos de información que se utilizan en los procesos de la empresa, adicionalmente debe tener una clasificación de acuerdo a su importancia y nivel de que debe poseer de acuerdo a la disponibilidad, integridad y confidencialidad, también se debe definir las propiedades de los activos como el propietario que es el encargado de establecer quien tiene acceso al activo y cuando la información ya no sea requerida determina el proceso que debe tener, el custodio técnico que es el encargado de administrar los controles de seguridad que requiera el activo como backups entre otros, siempre y cuando los defina el propietario y por ultimo está el usuario que es el que utiliza la información para su labor y de acuerdo a los permisos otorgados por el propietario puede tener acceso de lectura, escritura e incluso de modificación, entre otros[5].

2. Clasificar los activos de información

La clasificación de los activos de información es una parte fundamental, debido a que con este proceso la organización puede identificar los activos más críticos, para su funcionamiento, cada organización realiza este proceso de acuerdo a sus necesidades, pero lo más importante es basarse en los 3 pilares de la seguridad como lo son la integridad, disponibilidad y Confidencialidad, de acuerdo con la afectación de estos se definen los tipos de niveles de criticidad de los activos[6].

Tabla I. Clasificación activos

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

3. Gestión del riesgo

Este proceso consiste en identificar todos los riesgos asociados a los activos de información con un nivel de clasificación alto que son los más importantes para la organización, la priorización de los riesgos se da con base entre la probabilidad de que ocurra contra el impacto que genera[6].

Fig. 4. Priorización del riesgo, Obtenida de https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-organizaciones.pdf

El proceso de la administración del riesgo consta de las siguientes etapas, se debe establecer el contexto de la organización de acuerdo a los activos de información más críticos y definir los criterios que se utilizaran para evaluar la importancia de los riesgos[8].

Con base en la identificación de los activos se establecen las vulnerabilidades, amenazas y riesgos a los que se encuentran expuestos, se analizan y se evalúan mediante una matriz de riesgo lo que se busca con esta es visualizar los recursos de la organización e identificar los que poseen más riesgos de sufrir daños[9], para determinar los procesos o las acciones que se deben llevar a cabo como tratamiento del riesgo y los posibles controles que se deben realizar periódicamente para lograr llevar el riesgo a un nivel aceptable que las organizaciones están dispuestas a asumir, debido a que la mitigación del riesgo no puede ser al 100%, por ende siempre existirán riesgos cuyo impacto no sea tan devastador. Tan pronto finalice el proceso si se identifica todavía un riesgo muy alto, se puede volver a generar una segunda evaluación de riesgos como mecanismo de mejora continua y así sucesivamente hasta que se logre el nivel aceptable que la organización asuma para el funcionamiento de sus sistemas de información.

Fig. 5. Ejemplo matriz análisis del riesgo, Obtenida de https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

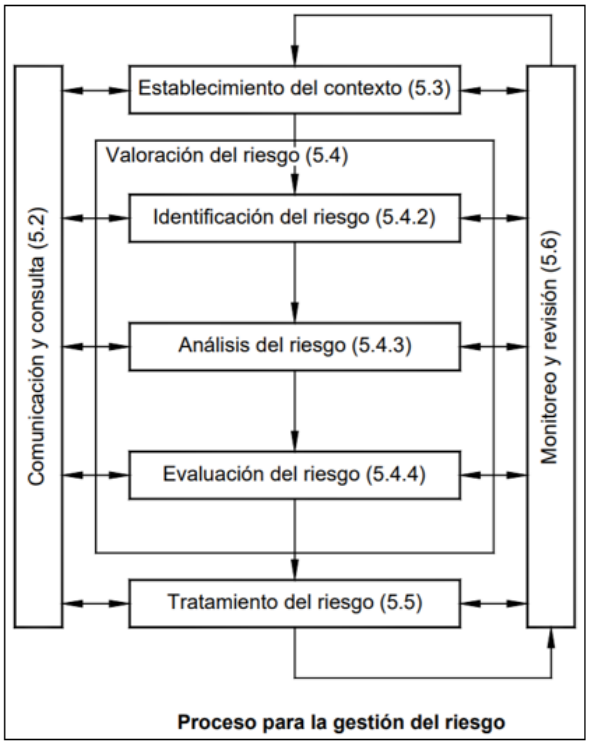

Fig. 6. Proceso de gestión del riesgo, Obtenida de NTC-ISO31000_Gestion_del_riesgo.

4. Plan de tratamiento del riesgo

En este punto del proceso es donde se establecen las medidas y controles necesarios para ayudar a reducir los riesgos a su mínima expresión, la reducción total del riesgo es muy poco probable que ocurra por lo tanto se genera un riesgo aceptable por la compañía y de tal caso de que se materialice este la compañía no tenga tantos efectos devastadores, algunos ejemplos de controles que pueden ser implementados son los siguientes:

- Acceso de usuarios a los sistemas mediante roles
- Políticas para la generación de contraseñas
- Antivirus
- Tarjetas de acceso a instalaciones físicas
- Políticas de Backup
- Políticas de almacenamiento de la información física y digital
- Cifrar los datos almacenados
- Firmas digitales
- Implementar un plan de capacitación a usuarios
- Plan de divulgación de los controles establecidos a todos los empleados de la organización

IV. DESARROLLO DEL PLAN DE CONTINUIDAD

Para proporcionar un modelo del plan de continuidad para los sistemas de información se hará referencia a la norma técnica NIST 800_34 que proporciona el instructivo de los

elementos que se deben de tener en cuenta a la hora de desarrollar un plan de continuidad.

Antes de iniciar con el plan de continuidad se debe realizar una adecuada gestión de riesgos y con el resultado de este se realizan los siguientes pasos para establecer el plan de continuidad que ayudara a minimizar los efectos en caso de que ocurra un fallo en la prestación del servicio.

1. Desarrollar la política del plan de contingencia

De acuerdo con el resultado de la gestión del riesgo en el cual ya se identificaron los activos de información que son más importantes para la organización y a los cuales se le aplicó el tratamiento de los riesgos quedando riesgos residuales, es en este punto donde se puede iniciar definiendo a que activos de información se le va aplicar el plan contingencia, los roles y las responsabilidades de las áreas involucradas, los recursos y las actividades que se van a contemplar en el desarrollo del plan, este se compone de directrices y procedimientos a realizar ante una interrupción del servicio sea por un desastre natural o por una intrusión de seguridad.

2. Análisis de Impacto de negocio BIA

La función de este mecanismo es realizar una validación entre los procesos de información críticos contra las consecuencias si se tuviera una interrupción del servicio, el tiempo mínimo requerido para reanudar la operación y los recursos que se necesitarían para esto, es decir establecer impacto de la interrupción y tomar las decisiones que se consideren para tener la afectación mínima posible, y también definir las prioridades de orden en el que se deben reestablecer los servicios de acuerdo a su nivel de criticidad [10].

3. Estrategias de recuperación y continuidad

Este proceso determina en primera instancia los activos de acuerdo a su nivel de importancia en cuanto a la disponibilidad del servicio esta parte se hace en la última fase del BIA y de acuerdo al resultado se establecen los tiempos que se pueden tolerar para que ocurra la recuperación de acuerdo a estos modelos de tiempo y una vez priorizados los servicios, se implementan las estrategias de recuperación y depende del análisis del BIA, si se generan planes de continuidad mientras ocurre la interrupción o se utilizan copias de respaldo, se evalúan lugares alternativos para contingencias o se utilizan sitios espejo para salvaguardar la disponibilidad de los servicios de información, en este punto se deben evaluar todas las posibles soluciones y el impacto tanto en costos como en tiempo que se requiere para llevar a cabos las actividades y perder el menor tiempo posible.

Es decir, en este punto del plan el proceso que se va a realizar debe ser capaz de garantizar que la continuidad del negocio y que los sistemas de información ante el fallo estén disponibles y si por algún motivo se llega al termino del incumplimiento de los niveles de servicio y cláusulas contractuales que puedan generar un impacto negativo en los recursos económicos de la organización el impacto sea lo más mínimo posible y que a la empresa le queden los recursos suficientes para afrontar este inconveniente.

Tabla II. Tiempos de recuperación

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

4. *Generación de Informe del plan de continuidad*

Después de realizadas las etapas anteriores se debe realizar un documento técnico donde se plasmen todas las actividades realizadas dentro del proceso, de esta manera se debe presentar un documento técnico con los listados de los servicios de información críticos, la prioridad que estos reciben, el tiempo de demora en la restauración y los procesos alternos que se realizan hasta que el servicio este reestablecido completamente. Adicionalmente en este documento se debe establecer la jerarquía de los equipos y las áreas que se involucran y empiezan a reaccionar ante una interrupción del servicio, adicionalmente en este documento debe quedar explicito cual es la ruta de comunicación entre los equipos, es decir a quien se debe informar y en qué momento.

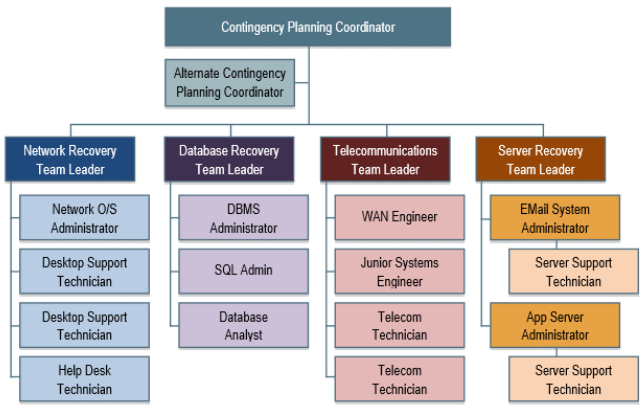

Fig. 7. Ejemplo de la jerarquía de un plan de continuidad , Obtenida de NIST Special Publication 800-34 Rev. 1

5. *Prueba del plan de continuidad y mejora continua*

Para que la definición del plan de continuidad sea efectiva y proporcione valor a la empresa, se debe tener una prueba controlada en un ambiente lo más real posible para poder

identificar si existen vacíos en alguna acción correctiva o si se puede presentar alguna situación que no se tenga contemplada para así de esta manera poderse adelantar a los inconvenientes que se presenten, debido a que es una prueba se pueden sacar provecho identificando futuras mejoras que se pueden implementar en un nuevo proceso como mejora al plan existente, es de vital importancia tener actualizado e informando a todas las personas que hacen parte de la organización. Este proceso de pruebas y mejora continua se recomienda que sea por lo menos una vez al año y que si por algún motivo la infraestructura de la empresa cambia o se realiza alguna actualización sobre los activos de información de la organización, automáticamente se debe evaluar si es necesario realizar actualización sobre el plan de continuidad existente.

V. CONCLUSIONES

Implementar en la compañía un sistema de gestión de riesgos ayuda a brindar la disponibilidad, integridad y confidencialidad de la información.

Implementar el plan de continuidad es una parte fundamental en el funcionamiento de los sistemas de información, para ayudar a soportar los servicios ante una interrupción.

Realizar el análisis de impacto del negocio ayuda a establecer los impactos que se pueden tener a la hora de una interrupción del servicio y los posibles efectos negativos que se generen.

La implementación de los controles que ayudan a mitigar los riesgos de los sistemas de información juega un papel fundamental en el plan de continuidad debido a que a partir de estos se implementa el plan de continuidad de las disponibilidad de los servicios ante la interrupción.

Actualizar el plan de continuidad del negocio es parte importante debido a que puede ayudar a evitar impactos económicos devastadores para la organización, debido a que los sistemas esta sufriendo actualizaciones constantemente y es importante que así mismo se actualice el plan de continuidad.

VI. REFERENCIAS

[1] Biblioteca Universidad Itson, «https://biblioteca.itson.mx,» [En línea]. Available: https://biblioteca.itson.mx/oa/dip_ago/introduccion_sistemas/p3.htm. [Último acceso: 24 11 2018].

[2] Izamorar, «https://izamorar.com,» [En línea]. Available: https://izamorar.com/actividades-basicas-de-un-sistema-de-informacion/. [Último acceso: 24 11 2018]

[3] Tipos de sistemas de información, «https://tiposdesistemasdeinformacion.wordpress.com,» [En línea]. Available: https://tiposdesistemasdeinformacion.wordpress.com/2015/04/09/sistema-de-procesamiento-de-transacciones-tps/. [Último acceso: 24 11 2018].

[4] Management information systems and accounting information system, «https://www.toppr.com,» [En línea]. Available: https://www.toppr.com/guides/accountancy/application-of-computers-in-accounting/management-information-systems-and-accounting-information-system/. [Último acceso: 25 11 2018].

[5] ISO 27001 Gestión Integral de la Seguridad de la Información, «https://www.novasec.co,» [En línea]. Available: http://www.novasec.co/blog/62-gestion-integral-de-la-seguridad-de-la-informacion. [Último acceso: 07 02 2019].

[6] Guía de gestion de riesgos, «https://www.mintic.gov.co,» [En línea] Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf. [Último acceso: 25 01 2019].

[7] El valor de la gestión de riesgos en las organizaciones, «https:// www.isotools.org,» [En línea] Available: https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-organizaciones.pdf. [Último acceso: 26 01 2019].

[8] Norma técnica colombiana NTC ISO/ 31000, Gestión del riesgo, principios y directrices. ICONTEC, NTC-ISO 31000, 2011. 34 p.

[9] Matriz para el Análisis de Riesgo, «https://protejete.wordpress.com,» [En línea] Available: https://protejete.wordpress.com/gdr_principal/matriz_riesgo/. [Último acceso: 08 02 2019].

[10] National Institute of Standards and Technology, Contingency planning guide for federal information systems, NIST 800-34 Rev. 1, 2010. 149 p.

Autor:
Diana Carolina Díaz Rodríguez Ingeniera de Sistemas de la Universidad Simón Bolívar Extensión Cúcuta, con experiencia de más de 5 años en el sector de las telecomunicaciones, Dando soporte a aplicaciones propias del cliente, formando parte de áreas de TI, Certificada en ITIL, participando en la elaboración de los acuerdos de servicio, soporte nivel 2 de la mesa de servicios y actualmente culminando estudios de postgrado como especialista en Seguridad informática en la universidad Piloto de Colombia.