Seguridad-Privada.net

SEGURIDAD INFORMATICA

Resumen—Este documento aborda la Seguridad Informática en España desde el prisma de la Ley de Protección de Datos (LOPD) y la normativa voluntaria UNE ISO/IEC 27001:2007.

I. Introducción

La Seguridad Informática está contemplada en la legislación española y en el marco de estándares y normativa específica, por lo que podemos abordar el tema desde la metodología y bajo el punto de vista legal.

La información es el principal activo de muchas organizaciones y precisa ser protegida adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio. En la actualidad, las empresas de cualquier tipo o sector de actividad se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de contingencias, las cuales pueden dañar considerablemente tanto los sistemas de información como la información procesada y almacenada. Ante estas circunstancias, las organizaciones han de establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio, primando la protección de la información.

Para proteger la información de una manera coherente y eficaz es necesario implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema es una parte del sistema global de gestión, basado en un análisis de los riesgos del negocio, que permite asegurar la información frente a la pérdida de:

- Confidencialidad: sólo accederá a la información quien se encuentre autorizado. Integridad: la información será exacta y completa.

- Disponibilidad: los usuarios autorizados tendrán acceso a la información cuando lo requieran.

La seguridad total es inalcanzable, pero mediante el proceso de mejora continua del sistema de seguridad se puede conseguir un nivel de seguridad altamente satisfactorio, que reduzca al mínimo los riesgos a los que se está expuesto y el impacto que ocasionarían si efectivamente se produjeran.

Los datos pueden alcanzar niveles de importancia no sólo de índole legal, económico o ético, sino que en algunos ámbitos protegiendo propia la información estamos protegiendo directamente instalaciones, tecnología, personas e incluso naciones. No hay límite al respecto.

II. Marco legal y estandarizado de la Seguridad Informática

En España existe normativa de obligado cumplimiento (Ley Orgánica de Protección de Datos), y varias normativas voluntarias, pero solo vamos a tratar la más importante y actualizada que es la ISO/IEC 27001:2005, que además es certificable por AENOR. Por el gran volumen de empresas certificadas, y por ser relativamente reciente, merece comentar tambien la norma UNE 71502:2004

II.1 UNE 71502:2004

Norma española certificable, desarrollada en base a BS7799-2:2002, que establece las especificaciones para los sistemas de gestión de seguridad de la información. Guarda relación con UNE-ISO/IEC17799:2002 mediante su Anexo A.

Elaborada por el comité técnico AEN/CTN 71 de la Tecnología de la Información, especifica **los requisitos para establecer, implantar, documentar y evaluar un SGSI dentro del contexto de los riesgos identificados por la organización**.

La publicación anticipada de ISO 27001 en el año 2005 acortó la vigencia de la norma española. Con la traducción al español de ISO 27001 y su publicación como UNE-ISO/IEC 27001, UNE 71502 quedó anulada en favor de la norma internacional a fecha 31 de Diciembre de 2008.

Aquellas empresas y organizaciones que hayan evolucionado según las prácticas señaladas por UNE 71502:2004 requieren de un esfuerzo mínimo para su reconocimiento internacional bajo la norma ISO 27001.

II.2 UNE ISO/IEC 27001:2007:

Desde el 28 Noviembre de 2007 está publicada en España. Se trata de una adaptación de la internacional ISO/IEC 27002:2005, publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

La redacción de esta norma es muy similar a la de ISO 9001, ISO 14001 y OHSAS 18001 con la intención de garantizar la posible integración de todos estos sistemas.

II.2.1 Definición de un SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significaque se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore.

La norma especifica que, como cualquier otro sistema de gestión, el SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Es decir, tanto la documentación de soporte como las tareas que se realizan. Los

sistemas de gestión que definen las normas ISO siempre están documentados, ya que, por un lado, es la mejor manera de formalizar normas e instrucciones y, por otro, son más fáciles de transmitir y comunicar, cosa que no sucedería si se confía en un traspaso de información verbal informal.

La norma es compatible con el resto de las normas ISO para sistemas de gestión (UNE-EN ISO 9001 y UNE-EN ISO 14001) y poseen idéntica estructura y requisitos comunes, por lo que se recomienda integrar el SGSI con el resto de los sistemas de gestión que existan en la empresa para no duplicar esfuerzos.

Incluso cuando no exista un sistema de gestión formal, el amplio conocimiento actual de estos sistemas hace que las principales características de la norma sean comprensibles para la mayoría de la gente, y que para explicarla en detalle sea suficiente con incidir en las diferencias fundamentales, a saber, que con un SGSI lo que tratamos es de gestionar la seguridad de la información de nuestra organización.

II.2.2 El ciclo de mejora continua

Para establecer y gestionar un sistema de gestión de la seguridad de la información se utiliza el ciclo PDCA (conocido también como ciclo Deming), tradicional en los sistemas de gestión de la calidad. El ciclo PDCA es un concepto ideado originalmente por Shewhart, pero adaptado a lo largo del tiempo por algunos de los más sobresalientes personajes del mundo de la calidad. Esta metodología ha demostrado su aplicabilidad y ha permitido establecer la mejora continua en organizaciones de todas clases.

El modelo PDCA o "Planificar-Hacer-Verificar-Actuar" (Plan-Do-Check-Act, de sus siglas en inglés), tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización:

- **Plan**. Esta fase se corresponde con establecer el SGSI. Se planifica y diseña el programa, sistematizando las políticas a aplicar en la organización, cuáles son los fines a alcanzar y en qué ayudarán a lograr los objetivos de negocio, qué medios se utilizarán para ello, los procesos de negocio y los activos que los soportan, cómo se enfocará el análisis de riesgos y los criterios que se seguirán para gestionar las contingencias de modo coherente con las políticas y objetivos de seguridad.

- **Do**. Es la fase en la que se implementa y pone en funcionamiento el SGSI. Las políticas y los controles escogidos para cumplirlas se implementan mediante recursos técnicos, procedimientos o ambas cosas a la vez, y se asignan responsables a cada tarea para comenzar a ejecutarlas según las instrucciones.

- **Check**. Esta fase es la de monitorización y revisión del SGSI. Hay que controlar que los procesos se ejecutan como se ha establecido, de manera eficaz y eficiente, alcanzando los objetivos definidos para ellos. Además, hay que verificar el grado de cumplimiento de las políticas y procedimientos, identificando los fallos que pudieran existir y, hasta donde sea posible, su origen, mediante revisiones y auditorías.

- **Act**. Es la fase en la que se mantiene y mejora el SGSI, decidiendo y efectuando las acciones preventivas y correctivas necesarias para rectificar los

fallos, detectados en las auditorías internas y revisiones del SGSI, o cualquier otra información relevante para permitir la mejora permanente del SGSI.

La mejora continua es un proceso en sí mismo. Debe entenderse como la mejora progresiva de los niveles de eficiencia y eficacia de una organización en un proceso continuo de aprendizaje, tanto de sus actividades como de los resultados propios.

Dado que la norma se encuentra enfocada hacia la mejora continua, es un esfuerzo innecesario tratar de implementar un SGSI perfecto en un primer proyecto de este tipo. El objetivo debería ser diseñar un SGSI que se ajuste lo más posible a la realidad de la organización, que contemple las medidas de seguridad mínimas e imprescindibles para proteger la información y cumplir con la norma, pero que consuma pocos recursos e introduzca el menor número de cambios posibles. De esta manera, el SGSI se podrá integrar de una forma no traumática en la operativa habitual de la organización, dotándola de herramientas con las que hasta entonces no contaba que puedan demostrar su eficacia a corto plazo.

La aceptación de este primer SGSI es un factor de éxito fundamental. Permitirá a la organización ir mejorando su seguridad paulatinamente y con escaso esfuerzo.

Esta norma especifica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica. Por ejemplo, uno de los principales requisitos es la realización de un análisis de riesgos con unas determinadas características de objetividad y precisión, pero no aporta indicaciones de cuál es la mejor manera de llevar a cabo dicho análisis. Puede ejecutarse con una herramienta comercial, con una aplicación diseñada expresamente para la empresa, mediante reuniones, entrevistas, tablas o cualquier otro método que se estime oportuno.

Todos estos recursos servirán para cumplir la norma, siempre y cuando se observen los requisitos de objetividad del método, los resultados sean repetibles y la metodología se documente.

II.3 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

El objeto de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos deCarácter Personal (en adelante LOPD), que derogó la antigua LORTAD de 1992, es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derecho fundamentales de las personas físicas, especialmente con la finalidad de preservar el honor, intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Todo esto es aplicable a los datos de carácter personal registrados en cualquier tipo de soporte físico susceptible de ser tratado (ya sea informático o manual).

Por lo tanto, con motivo de la entrada en vigor de la LOPD surgen una serie de obligaciones para aquellas organizaciones que posean ficheros con datos de carácter personal.

La Constitución Española establece en su artículo 18 el derecho a la intimidad de las personas cuando dice:

"*18.1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*

18.4. La Ley limitará el uso de la Informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

En el presente documento vamos a abarcar la parte de la Ley concerniente a las obligaciones y requerimientos de seguridad informática, dejando fuera de alcanze otros aspectos como faltas y sanciones.

II.3.1 Obligaciones legales básicas de la normativa de protección de datos

- **Calidad de los datos**: los datos de carácter personal solo se podrán recoger para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, no podrán usarse para otras finalidades incompatibles con aquellas, serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado y serán cancelados cuando hayan dejado de ser necesarios o pertinentes. (Art.4)

- **Deber de Secreto**: El Responsable del Fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero. (Art.19)

- **Información en la recogida de datos**: Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del Responsable del Fichero. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos estas advertencias en forma claramente legible. (Art.5)

- **Consentimiento del afectado**: El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas, sean necesarios para un contrato o figuren en fuentes accesibles al público. Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Estos y los datos sobre origen racial, salud o vida sexual solo pueden ser recogidos, tratados o cedidos, con el consentimiento

expreso y por escrito del afectado. Sin embargo, estos tipos de datos sí podrán tratarse, cuando resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario o equivalente, sujeto al secreto profesional. (Art.6-7)

- Sin perjuicio de lo que se dispone en el artículo 11 de la LOPD respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad. (Art.8)

- **Comunicación o cesión de datos**: Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado. Sin embargo este consentimiento no será preciso cuando la cesión está autorizada en una Ley, o cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica (cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros), o cuando los datos procedan de fuentes accesibles al público, o cuando la cesión sea de datos relativos a la salud y sea necesaria para solucionar una urgencia (que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica), o cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. (Art.11)

- **Inscripción de los ficheros** en el Registro General de la Agencia Española de Protección de Datos (RGPD), con previa publicación en Boletín Oficial de una Disposición General con la declaración de los ficheros. (Art.20)

- **Tutela del derecho de los afectados de acceso, rectificación y cancelación**, estableciendo el procedimiento interno apropiado. (Art.15-16-17)

- **Redacción e implantación del documento de seguridad** que incluya toda la normativa de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad de los datos objeto de tratamiento. Será de obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de información. (Art.9)

- **Auditoría** cada dos años del cumplimiento de la legislación y de los procedimientos de seguridad. (Art.96)

- **Auditoría** cada dos años del cumplimiento de la legislación y de los procedimientos de seguridad. (Art.110)

II.3.2 Documento de Seguridad

Entre las medidas que aprobó la LOPD se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

La Ley no define extrictamento el contenido del "Documento de Seguridad" , pero propone un modelo organizado en dos partes: en la primera se recogen las medidas que afectan a todos los sistemas de información de forma común, y en la segunda se incluye un anexo por cada fichero o tratamiento, con las medidas que le afecten de forma específica. Apróximadamente el documento tendría la siguiente forma:

El contenido principal de este Documento queda estructurado como sigue:

- Ámbito de aplicación del documento.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
- Procedimiento general de información al personal.
- Funciones y obligaciones del personal.
- Procedimiento de notificación, gestión y respuestas ante las incidencias.
- Procedimientos de revisión.
- Consecuencias del incumplimiento del Documento de Seguridad.
- Anexos I. Aspectos específicos relativos a los diferentes ficheros.
- Anexo II. Nombramientos
- Anexo III. Autorizaciones firmadas para la salida o recuperación de datos
- Anexo IV. Inventario de soportes (si se gestiona en papel)
- Anexo V. Registro de Incidencias (si se gestiona en papel)
- Anexo VI. Contratos o cláusulas de encargados de tratamiento (si existen, de acuerdo con lo indicado en el artículo 12 de la LOPD).
- Anexo VII: Registro de entrada y salida de soportes

Este Documento deberá mantenerse permanente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

II.4 R.D. 1720/2007 (Reglamento de desarrollo de protección de datos de Carácter Personal)

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, identifica tres niveles de medidas de seguridad, básico, medio y alto, los cuales deberán ser adoptados en función de los distintos tipos de datos personales de los que se disponga en cada fichero:

Nivel	Tipos de Datos	Medidas Seguridad Obligatorias
Básico	▪ Afecta a todos los ficheros que contengan datos personales ▪ Nombre ▪ Apellidos ▪ Direcciones de contacto (tanto físicas como electrónicas) ▪ Teléfono (tanto fijo como móvil) ▪ Otros	▪ Documento de seguridad ▪ Régimen de funciones y obligaciones del personal ▪ Registro de incidencias ▪ Identificación y autenticación de usuarios ▪ Control de acceso ▪ Gestión de soportes ▪ Copias de respaldo y recuperación
Medio	▪ Comisión infracciones penales ▪ Comisión infracciones administrativas ▪ Hacienda Pública ▪ Servicios financieros ▪ Información sobre solvencia patrimonial y crédito	▪ Medidas de seguridad de nivel básico ▪ Responsable de Seguridad ▪ Auditoría bienal ▪ Medidas adicionales de Identificación y autenticación de usuarios ▪ Control de acceso físico ▪ Medidas adicionales de gestión de soportes. ▪ Registro de incidencias. ▪ Pruebas sin datos reales
Alto	▪ Ideología ▪ Religión ▪ Creencias ▪ Origen racial ▪ Salud ▪ Vida sexual ▪ Datos recabados para fines policiales sin consentimiento de las personas afectadas	▪ Medidas de seguridad de nivel básico y medio ▪ Seguridad en la distribución de soportes ▪ Registro de accesos ▪ Medidas adicionales de copias de respaldo ▪ Cifrado de telecomunicaciones

II.4.1 Obligaciones legales

- Establece la obligación a todas las organizaciones de poner en marcha las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la LOPD.

- Tratamiento por cuenta de terceros: deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el Encargado del Tratamiento únicamente tratará los datos conforme a las instrucciones del Responsable del Fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, el Reglamento de desarrollo del RD 1720/2007 que el Encargado del Tratamiento está obligado a implementar.

- Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al Responsable del Fichero, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. En el caso de que el Encargado del Tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

III. Plan de continuidad de negocio (BCP[1])

Un BCP son el conjunto de aspectos técnicos y organizativos que permiten a las organizaciones continuar su actividad en la situación de que un evento afecte sus operaciones, bien mediante la recuperación de los procesos de soporte o mediante la aplicación de procesos de emergencia. Es fundamental un análisis del impacto económico (BIA[2]) que tendría sobre la empresa cualquier eventualidad.

Por ejemplo, en el atentado del 11 de septiembre del 2001, varias empresas fracasaron por la falta de un plan de continuidad del negocio. Esto creó la necesidad de que actualmente las organizaciones estén implementando mecanismos y/o técnicas, que mitiguen los riesgos a los que se está expuesto, brindando una alta disponibilidad en las operaciones de su negocio.

Un plan de continuidad afecta tanto a los sistemas informáticos como al resto de procesos de una organización y tiene en cuenta la situación antes, durante y después de un incidente.

Una de las recomendaciones para mitigar los riesgos es la necesidad de recuperar los recursos, ya sean humano, infraestructura, datos vitales, tecnología de información, equipos de oficina e implementos requeridos que permitan continuar con el funcionamiento normal de la organización.

No hay que confundir un BCP, con un Plan de Recuperación contra desastres (DRP[3]). El segundo se centra en realizar exclusivamente planes de prevención y recuperación antes los escenarios de desastre con mayor impacto y probabilidad de ocurrencia en el ámbito de los sistemas de información de la organización. En un DRP son críticos los tiempos de pérdida y recuperación de información.

Un BCP se considera una parte clave en la implantación de un SGSI. En la norma UNE-ISO/IEC 27001 de Sistemas de Gestión de Seguridad de la Información hace referencia a la Gestión de la continuidad desde el punto de vista del negocio propio y de la seguridad de la información.

---

[1] BCP, en ingles: Business Continuity Plan (Plan continuidad de negocio)

[2] BIA, en inglés: Business Impact Analysis (Análisis de impacto)

[3] DRP, en ingles: Disaster Recovery Plan (Plan de recuperación de desastres)

El Desarrollo del BCM básicamente se centra en recopilar la información necesaria para entender el negocio.

Para la implementación del BCM en una organización se deben tener en cuenta varios estados o fases que son necesarias para el funcionamiento eficaz y ágil de las actividades en una empresa.

La realización del BCM en la organización traerá grandes ventajas como por ejemplo:

- Administrar la continuidad del negocio
- Resistencia del negocio ante interrupciones
- Protege y asegura la imagen de la empresa
- Abre nuevas oportunidades de mercado y ayuda a ganar nuevos negocios.
- Aumenta la disponibilidad del negocio.

El desarrollo de un BCM en la organización permitirá estar preparados para afrontar situaciones de interrupción de sus procesos críticos.

Un BCM involucra todos los recursos de la organización. Por lo cual con su realización analizaremos y podremos establecer estrategias que garanticen una continuidad del negocio, buscando minimizar la dependencia de los recursos con lo que cuenta la empresa (IT, Humano, infraestructura, Económicos, etc) brindando una alta disponibilidad de los servicios ofrecidos

III.1 Fases para la implementación de un BCM

III.1.1 Inicio y gestión del proyecto

El objetivo es establecer la necesidad de desarrollar el BCM en la organización, de tal manera que se comunique la importancia de realizar este plan, involucrando a los directivos y el personal de la empresa.

III.1.2 Evaluación y control del riesgo

El objetivo de la evaluación de riesgos es identificar las amenazas internas y externas, incluyendo concentraciones de riesgo, que pueden causar la interrupción o pérdida de la Actividades Críticas de una organización, así como la probabilidad (o frecuencia) de que ocurra una amenaza y cómo es vulnerable una organización a varios tipos de amenazas permitiendo su gestión de priorización y control para formar una base en la que se establezca un programa de control y un plan de acción de gestión de riesgo.

Para realizar una evaluación y control de riesgos se debe tener en cuenta lo siguiente:

- Identificar riesgos
- Análisis/Evaluación de riesgos

- Gestión y Control de riesgos

Después de realizar la evaluación y el control de riesgos, los resultados obtenidos incluyen la identificación y documentación de:

- La probabilidad de ocurrencia, en la organización, a un tipo específico de amenaza.
- Concentración de riesgos donde el número de Actividades de Misión Crítica es localizado dentro del mismo edificio o en el mismo lugar.
- Una evaluación y análisis de riesgos (combinado con un Análisis de Impacto del Negocio - BIA).
- Una estrategia de gestión de control de riesgo y plan de acción.
- El enfoque de priorización del BCM y control de riesgos.

III.1.3 Análisis de impacto del negocio (BIA).

El Análisis de Impacto del Negocio (BIA – Business Impact Analysis) consiste en técnicas y metodologías que pueden ser usadas para identificar, cuantificar y cualificar los impactos de negocio y sus efectos en una organización en caso de pérdida o interrupción de las Actividades de Misión Crítica. Sin embargo, la clave para realizar un Análisis de Impacto del Negocio es analizar el negocio como un todo más no como componentes, procesos o funciones individuales.

El análisis BIA tiene en cuenta el RTO (Recovery Time Objective) y RPO (Recovery Point Objective) que deben ser establecidos por la organización. Están definidos como:

- RTO (recovery Time Objective): El tiempo entre el punto de interrupción, y el punto en el cuál los sistemas sensibles en el tiempo deben estar funcionando nuevamente, con los datos actualizados.
- RPO (Recovery Point Objective): El punto en el cuál fueron interrumpidas las actividades del sistema debido a la ocurrencia de un determinado evento.

El objetivo de un Análisis de Impacto del Negocio es identificar las actividades de misión crítica de una organización, sus dependencias y sus puntos de fallas así como analizar el impacto y el efecto que se generaría en caso de la perdida e interrupción de las actividades de misión crítica. A su vez, informar y permitir opciones para crear una resistencia en las operaciones de negocio de la organización.

III.1.4 Desarrollo de estrategias para la continuidad del negocio.

El propósito del desarrollo de estrategias consiste en identificar las alternativas de recuperación de las operaciones en los marcos de tiempo definidos.

El desarrollo de las estrategias del BCM involucra los siguientes aspectos:

- Identificar los requerimientos de continuidad de la organización.
- Evaluar la compatibilidad de las estrategias contra los resultados del BIA.
- Presentar el análisis costo / beneficio de las estrategias de continuidad.
- Seleccionar los sitios alternos y de almacenamiento externo.
- Entender los términos contractuales de los servicios de continuidad del negocio.

Algunas de las alternativas de recuperación comprenden estrategias de almacenamiento externo a la organización (Ej. Hotsite, coldsite, etc.), a su vez procedimientos de recuperación interna documentados, así como acuerdos recíprocos entre empresa-empresa y/o empresa-cliente, o una utilización de combinación de estrategias.

III.1.5 Respuesta ante emergencias.

El propósito de la fase de respuesta ante emergencias es desarrollar e implementar procedimientos para responder y estabilizar la situación después de un incidente y administrar el centro de operaciones de emergencia a ser utilizado como "centro de mando".

Para cumplir con este propósito es necesario que:

- Identifique componentes de los procedimientos de respuesta a emergencia.
- Especifique los procedimientos de respuesta a emergencia.
- Identifique requerimientos de control y autoridad.
- Procedimientos de control y autoridad.
- Respuesta a emergencia y recuperación de heridos.
- Seguridad y recuperación.

III.1.6 Desarrollo e implementación del BCM.

Esta fase involucra el diseño, desarrollo e implementación de planes de continuidad del negocio para evitar interrupciones de acuerdo a los marcos establecidos por los RTO'S y RPO'S.

- Un buen desarrollo e implementación de un BCM incluye:
- Identificar requerimientos para el desarrollo de los planes.
- Definir requerimientos de control y administración de la continuidad.
- Identificar y definir un formato y la estructura principal de los componentes de los planes.
- Elaborar un borrador de los planes.

- Definir procedimientos de gestión de crisis y continuidad del negocio.
- Definir las estrategias de evaluación de daños y reanudación.
- Desarrollar una introducción general a los planes.
- Desarrollar la documentación de los equipos de operación del negocio.
- Desarrollar la documentación de los equipos de recuperación de tecnología de información.
- Desarrollar el sistema de comunicaciones.
- Desarrollar los planes de los usuarios finales de aplicaciones.
- Implementar los planes.
- Establecer los procedimientos de control y distribución de los planes.

III.1.7 Programa de concientización y capacitación.

Toda organización que quiera posicionarse en el mercado y estar preparada a cambios en su entorno, requiere de un constante proceso de evolución. Este proceso genera en la mayoría de los casos, cambios al interior de la empresa. Siempre que se presentan estos cambios existe un porcentaje de resistencia al cambio relacionado con el personal que interviene en dicho proceso.

Es necesario que la organización prepare a sus empleados ante la presencia de un cambio, logrando minimizar esa resistencia y obteniendo mejor disposición ante situaciones de este tipo creando una cultura de aceptación ante un evento que perturbe su labor.

Son estos algunos motivos por los cuales se presenta en la gestión de continuidad de negocio una fase en la cual se trata la concientización y entrenamiento del BCM y su relación con la implementación mantenimiento, gestión y ejecución del mismo. Este proceso de conciencia es necesario que se realice en toda la organización (no solamente en el área de IT) logrando aumentar la resistencia ante riesgos.

Para logran una concientización y entrenamiento en necesario:

- Definir objetivos de concientización y entrenamiento
- Desarrollar e implementar varios tipos de programas de entrenamiento
- Desarrollar programas de concientización
- Identificar otras oportunidades de educación

III.1.8 Mantenimiento y ejercicio del BCM.

Una vez se han declarado y documentado estas estrategias y planes, que contribuyen al proceso de normalización ante una situación de crisis, es necesario realizar pruebas para determinar la eficacia con la que puede continuar el negocio

ante la presencia de una posible interrupción. Así mismo se puede evaluar el equipo y personal a cargo de cada actividad crítica, además se realizara una prueba al sistema demostrando competencia y capacidad de continuidad de negocio.

Los resultados que se obtendrán con el proceso de mantenimiento son de gran utilidad para la organización, previniendo que los documentos realizados queden obsoletos con el paso de los años. Para realizarlo es necesario tener una clara definición y documentación del programa de mantenimiento y monitoreo, incluyendo políticas, marcos y procesos así como la estrategia de negocio operacional.

La tecnología de información IT es un gran apoyo en los proceso de una organización, es necesario que se realice un análisis de la tecnología requerida por la organización cuando se tienen interrupciones en el sistema, para este punto el estándar ISO 17999 el cual trata sobre la seguridad de IT será de gran ayuda.

Para la realización de cualquier plan es necesario tener en cuenta la legislación existente, para tener una base y cumplir con la normatividad que se exige.

El proceso de mantenimiento requiere de un subconjunto de procesos auditoria ejercicio y aseguramiento que permiten su fortalecimiento, capacidad de continuidad y soporte a la gestión de continuidad de negocio en su aplicación a la organización cuando lo requiera.

III.1.9 Comunicación de crisis.

La etapa de comunicación de crisis se propone desarrollar, coordinar, evaluar y ejercitar planes para comunicarlos a directivos, personal, usuarios, proveedores y medios de comunicación, de tal forma que el entorno de la organización se entere de su estado y en caso de crisis poder reaccionar de forma adecuada para minimizar los costos de interrupción de los procesos internos.

Para ello, el BCM debe contener un listado de clientes, proveedores y medios de comunicación entre otros, en el cual se muestren los datos básicos de cada contacto.

III.1.10 Coordinación con Autoridades públicas.

En esta etapa se quiere que la organización tenga una clara definición y documentación de las políticas a implementar como un documento obligatorio en la organización. Por lo tanto, en este proceso la organización vera los resultados en la mejoría de los procesos de toda su organización, teniendo en cuenta que las políticas están dirigidas a la organización como un todo.