## Lecturas recomendadas

Se presentan a continuación varias direcciones de artículos con una breve descripción del contenido que en ellas se trata las cuales se consideran de interés en materia de Continuidad del Negocio.

**Direcciones electrónicas con Artículos relacionados con “Continuidad del Negocio”**

* <http://www.networkworld.es/Las-7-mejores-practicas-de-seguridad/seccion-/articulo-182238>

***“Las 7 mejores prácticas de seguridad”*** Si se implementan, con toda seguridad se percibirá una rápida mejora en el tiempo de operación, rendimiento y estado de conformidad de las TI de cualquier empresa.

* <http://www.channelplanet.com/index.php?idcategoria=12410>

***“Las empresas siguen concentrando sus planes de continuidad del negocio en torno a su capacidad de Tecnologías de Información (IT)”***Las empresas siguen concentrando sus planes de continuidad del negocio en torno a su capacidad de Tecnologías de Información (IT) Las empresas siguen concentrando sus planes de continuidad del negocio en torno a su capacidad de Tecnologías de Información (IT)

¿Cuáles son las causas del cese de actividades de una organización?

¿Cuántas empresas tienen un plan de continuidad del negocio?

De acuerdo con una encuesta realizada por The Chartered Management Institute en enero de este año las empresas que tienen un plan de continuidad de negocios en sus organizaciones concentran sus planes en torno a ciertos tipos de interrupciones como la pérdida de capacidad IT (87%) - la cual se refiere a problemas en el flujo y procesamiento normales de la información - pese a tener conocimiento del amplio rango de amenazas en otras unidades funcionales de la organización que pueden afectar sus negocios.

* <http://dialnet.unirioja.es/servlet/articulo?codigo=2063931>

***“Auditoría de Sistemas de Información y Planes de Continuidad del Negocio”***

Autores: Agatino Grillo

Localización: Novática: Revista de la Asociación de Técnicos de Informática, ISSN 0211-2124, Nº. 166, 2003 (Ejemplar dedicado a: Planes de contingencia TIC y continuidad de negocio), págs. 10-14

Resumen:

Un Plan de Continuidad del Negocio (PCN) es responsabilidad de la Dirección de la empresa. La auditoría del PCN es un elemento fundamental para la gobernación de las Tecnologías de la Información (TI) pues representa una opinión independiente cuyos resultados puede ser compartidos con, y comunicados a los implicados en dicha gestión, las autoridades reguladoras, o los socios de negocio. En particular, las auditorías del PCN son obligatorias legalmente para las instituciones financieras. Por todo ello es necesario adoptar una metodología PCN bien estructurada y verificable. Este artículo introduce la problemática general de la Auditoría de los Sistemas de Información (ASI --Information Systems Auditing, ISA) y presenta una aproximación al PCN basada en COBIT (Control Objectives for Information and Related Technology), un marco general desarrollado por ISACA (Information Systems Audit and Control Association).

* <http://www.segurilatam.com/actualidad/editoriales-y-tribunas/esta-preparado-para-enfrentar-una-crisis-disene-su-plan-de-continuidad-de-negocio>

**¿Está preparado para enfrentar una crisis? Diseñe su plan de continuidad de negocio**

Cuando en las empresas hablamos sobre la continuidad del negocio, lo primero que debemos tener presente es que después de enfrentar una crisis sólo hay cabida para dos tipos de compañías: las que salen adelante y, en consecuencia, fortalecidas y las que no pueden recuperarse rápidamente e incluso cesan sus operaciones.

Seguramente, el primer grupo de organizaciones cuenta con procesos claros, debidamente documentados, y se ha preparado para el manejo de incidentes, de diverso origen y consecuencias, establecidos en lineamientos de continuidad del negocio. Estas guías están lideradas desde la gerencia sénior y han sido definidas como de alta prioridad.

* <http://www.sisteseg.com/files/Microsoft_PowerPoint_-_PLANES_DE_CONTINUIDAD_NEGOCIO_V_3.0.pdf>

***“Plan de Continuidad para el Negocio”*** Presentación que contiene los elementos que integran un Plan de Continuidad para el Negocio.

* <http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no127/item/134-cultura-de-seguridad-de-la-informaci%C3%B3n>

**EDITORIAL. CULTURA DE SEGURIDAD DE LA INFORMACIÓN**

Custodio de la ventaja competitiva empresarial.. Hablar de una cultura de seguridad de la información en el contexto de una sociedad altamente conectada, de información instantánea, con movilidad permanente y exigente de nuevos servicios tecnológicos, es hablar de un blanco móvil en un escenario dinámico; es decir, el desafío de crear valor desde la protección de los activos de información, haciendo parte de las exigencias de los mercados emergentes donde la velocidad de ingreso, la oportunidad del producto y las ventajas superiores de los servicios marcan la diferencia, cuando de crear una experiencia diferente se trata.

* <http://www.welivesecurity.com/la-es/2014/01/06/iso-22301-2012-estandar-continuidad-negocio/>

**ISO 22301:2012 el estándar de la continuidad del negocio**

Como parte de la gestión de la seguridad de la información es muy importante tener un plan de contingencia para garantizar la continuidad del negocio. El estándar certificable y auditable ISO 22301:2012, puede utilizarse como guía para establecer un modelo que garantice la seguridad de la información en caso de una emergencia.

* <http://www.welivesecurity.com/la-es/2015/12/30/5-consejos-mitigar-un-incidente-seguridad-empresa/>

**5 consejos para mitigar un incidente de seguridad en la empresa**

En el ámbito de la seguridad informática, muchas veces suele decirse que existen dos clases de empresas: las que han sido atacadas y las que serán atacadas. Normalmente, cuando una organización es víctima de un primer ataque informático se genera un estado de pánico y una sensación de incertidumbre.

* <http://www.welivesecurity.com/la-es/2015/12/29/resiliencia-operativa-infraestructura-critica/>

**Cómo aplicar la resiliencia operativa en infraestructura crítica**

En un ambiente dinámico, los cambios externos ponen a prueba la capacidad de los sistemas para recuperar su estado inicial (que en ocasiones también es el estado ideal), luego de que finaliza alguna perturbación a la cual habían estado sometidos. Esta propiedad es conocida como resiliencia, misma que puede ser aplicada en diferentes ambientes.

* <http://www.welivesecurity.com/la-es/2012/10/22/10-pilares-basicos-norma-iso27001/>

**Los 10 pilares básicos de la norma ISO 27001**

En la búsqueda del mejor estándar para gestionar la seguridad de la información en una compañía, generalmente los resultados suelen están alrededor de la serie de normas ISO 27000 ya que reúne todos los lineamientos en materia de gestión de seguridad de la información. Una de las normas más importantes, que además es certificable, es la ISO 27001, la cual está organizada en 11 dominios. A continuación vamos a tratar 10 de ellos, pues en un post anterior mencionamos lo que se debe tener en cuenta en la política de seguridad de la información, el undécimo de los dominios de esta norma.

* <http://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/>

**4 pasos para armar un Plan de Continuidad del Negocio**

Cuando hablamos de continuidad del negocio nos referimos a la capacidad de sobrevivir a las “cosas malas” que pueden tener un impacto negativo en la empresa: desde un brote de virus informático hasta un brote de virus biológico, y todos los demás peligros entre ambos, como incendios, inundaciones, tornados, huracanes, terremotos y tsunamis. El estándar internacional para la continuidad del negocio, ISO 22301, la define como la “capacidad [de una organización] de continuar la prestación de productos o servicios en los niveles predefinidos aceptables tras incidentes de interrupción de la actividad”.

* <http://www.welivesecurity.com/la-es/2012/07/18/continuidad-negocio-como-responder-ante-emergencia/>

**Continuidad del negocio: ¿cómo responder ante una contingencia?**

Cuando se habla de gestionar la seguridad de la información en la empresa, lo primero que se viene a la mente son dispositivos para protección de la red de datos, sistemas contra códigos maliciosos, contraseñas seguras, control de acceso, restricción del uso de dispositivos removibles y otra cantidad de políticas, procedimientos y tecnologías con el objetivo de garantizar que la información de la empresa estará a salvo en condiciones normales de operación. Pero, ¿se encuentra preparada la empresa para afrontar una situación de contingencia garantizando condiciones aceptables de operación y la seguridad de la información?.

* <http://www.welivesecurity.com/la-es/2013/08/13/necesidad-revision-periodica-riesgos-empresas/>

**La necesidad de la revisión periódica de los riesgos en las empresas**

Tener claramente identificadas en una empresa cuáles son las razones por las cuales se puede llegar a materializar un riesgo es importante para saber cuál es la mejor forma de hacerle frente. Veamos a continuación los conceptos sobre los que debe tenerse mayor claridad para identificar un riesgo.

* <http://www.welivesecurity.com/la-es/2013/03/19/consejos-mejorar-plan-respuesta-incidentes/>

**Consejos para mejorar el Plan de Respuesta a Incidentes**

Después de tener formulado el Plan de Continuidad del Negocio para saber cómo responder ante una contingencia es necesario tener en cuenta algunas actividades periódicas que van a ayudar a que la empresa esté preparada para enfrentar algún incidente.

* <http://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/>

**COBIT para la seguridad en las organizaciones**

Cuando hablamos de la protección de la información en las organizaciones, no importa si nos referimos a empresas públicas o privadas, grandes o pequeñas, lucrativas o no, ya que cada una de ellas tiene un objetivo primordial, que se ve reflejado en su misión, su razón de ser.

Para lograrla, llevan a cabo múltiples tareas que conducen hacia este propósito, al tiempo que se evitan otras acciones que impidan su cumplimiento. En este escenario toma relevancia la información, un recurso clave desde el momento en el que es creada hasta su destrucción, de manera que sea posible evadir las amenazas que pudieran afectarla.

* <http://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/>

**¿Cuál es la idea central de aplicar ISO 27001?**

El ambiente dinámico de los riesgos de seguridad nos muestra cambios continuos, donde nuevas amenazas son desarrolladas, vulnerabilidades son descubiertas e incidentes de seguridad se presentan con repercusiones importantes, tanto para empresas como para los individuos. Un enfoque se centra en la idea de que ante este escenario, solo es cuestión de tiempo para padecer las consecuencias de dichas amenazas.

* <http://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/>

**Business Impact Analysis (BIA) y la importancia de priorizar procesos**

El análisis de impacto al negocio (Business Impact Analysis o BIA por sus siglas en inglés) es otro elemento utilizado para estimar la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre.

A diferencia de una evaluación de riesgos, que se enfoca en cómo podría verse afectada una organización a través de la identificación, análisis y valoración de amenazas de seguridad con base en su impacto sobre los activos críticos y la probabilidad de ocurrencia, el BIA es un proceso más especializado en la identificación de los tipos de impacto, orientado en conocer qué podría verse afectado y las consecuencias sobre los procesos de negocio.