



## PLAN DE SEGURIDAD DE BASES DE DATOS APLICADO A GOBIERNOS AUTONOMOS DESCENTRALIZADOS

**Saltos Viteri Harry Adolfo<sup>1</sup>**

GAD Provincial de Los Ríos

[hsaltos@los-rios.gob.ec](mailto:hsaltos@los-rios.gob.ec)

**Santos Franco Gladys Isabel<sup>2</sup>**

Hospital General Babahoyo (IESS)

[santosgladys2009@hotmail.com](mailto:santosgladys2009@hotmail.com)

**Dávila Santillán Lisbeth Narcisa<sup>3</sup>**

Universidad de las Artes (UArtes)

[lisbeth.davila@uartes.edu.ec](mailto:lisbeth.davila@uartes.edu.ec)

Para citar este artículo puede utilizar el siguiente formato:

Saltos Viteri Harry Adolfo, Santos Franco Gladys Isabel y Dávila Santillán Lisbeth Narcisa (2017): "Plan de seguridad de bases de datos aplicado a Gobiernos autónomos descentralizados.", Revista Caribeña de Ciencias Sociales (septiembre 2017). En línea: <http://www.eumed.net/rev/caribe/2017/09/seguridad-datos-gobiernos.html>

### RESUMEN

Hasta el presente en las organizaciones es vital la implementación de ambientes seguros que garanticen y protejan la información, la base de datos del negocio no debe ser vulnerada por ninguna circunstancia, es así que este documento está preparado para aportar como Plan de Seguridad. Se han establecido parámetros que permitirán reducir riesgos y vulnerabilidades, sin dejar descuidado su entorno, es decir que también hay que asegurar el lugar donde se aloja, desde donde se accede, quienes son los que acceden y qué roles deben de tener para su acceso; también la disponibilidad de que esta pueda recuperarse de fallas en tiempos prudentes de forma automática o a través de la preparación de planes de recuperación guiados; el tener un eficiente fluido eléctrico ininterrumpido, provisto desde UPS y Generadores eléctricos. Se han incorporado controles extraídos de estándares probados que han tenido madurez y buenas prácticas en otros lugares, esto el ISO 27001, con su anexo 27002, para reaccionar e identificar de la mejor manera los riesgos que existen en las organizaciones, para garantizar la puesta en marcha de estos controles debe ir netamente apegada a una política informática institucional.

**Palabras claves:** Seguridad – Bases de Datos- Información – Riesgo - ISO 27001.

### ABSTRACT

Until the present in the organizations is vital the implementation of secure environments that guarantee and protect the information, the database of the business should not be violated by any circumstance, so this document is prepared to contribute as a Security Plan. We have established parameters that will allow us to reduce risks and vulnerabilities, without neglecting their environment, that is to say, we must also ensure the place where they are located, where they are accessed, who are the ones who access and what roles they must have for their

<sup>1</sup> Magister en Ingeniería y Sistemas de Computación. Especialista en Auditoria de Sistemas de Información. Magister en Dirección de Empresas con Énfasis en Gerencia Estratégica. Coordinador de TICs en el GADP Los Ríos. Maestro de Tecnologías en la Universidad Técnica Babahoyo.

<sup>2</sup> Ingeniera en Sistemas, graduada en la Universidad Técnica Babahoyo. Tecnólogo en Informática - Análisis De Sistemas en el Instituto Tecnológico Superior Babahoyo. Oficinista en el Hospital General Babahoyo (IESS).

<sup>3</sup> Ingeniera en Sistemas, graduada en la Universidad Técnica Babahoyo. Egresada de la Maestría de Tecnología e Innovación Educativa en la Universidad Casa Grande. Docente del Departamento de Nivelación de la UArtes.

access; Also the availability that it can recover from failures in prudent times automatically or through the preparation of guided recovery plans; To have an efficient uninterrupted electric fluid, provided from UPS and Electric generators. Controls extracted from proven standards that have had maturity and good practices in other places have been incorporated, this is ISO 27001, with its annex 27002, to react and identify the risks that exist in the best of the organizations, to ensure the of these controls must be clearly attached to an institutional information policy.

**Keywords:** Security - Databases - Information - Risk - ISO 27001.

## **1. INTRODUCCIÓN**

Desde la perspectiva más general la evolución tecnológica ha llevado a las empresas a considerar que las TIC's desempeñan un rol estratégico para su desarrollo y que la información procesada por los usuarios de computadoras es un insumo para lograrla transformar en servicios y productos que luego servirán de generadoras de beneficios importantes.

Si bien es cierto todas las organizaciones que operan con recursos tecnológicos se ven sumergidas en ambientes agresivos y hostiles, que pueden enfrentar acciones, como robo de información, sabotaje, entre otros; por lo que es de vital importancia que éstas cuenten con esquemas preventivos de seguridad informática que les permita disponer de los medios necesarios para contrarrestar amenazas, tanto desde el interior como del exterior de la organización, para así mantener su base de datos salvaguardada y con disponibilidad de la información para producir y tomar decisiones.

Varias empresas piensan que disponen de una correcta Seguridad Informática y creen que sus "datos confidenciales" son inaccesibles a personal no autorizado; pero el hecho es que en la mayoría de casos, al fin de mes o de año, las empresas competidoras disponen en la Mesa de Reuniones los balances generales de estas "empresas con políticas de Seguridad Informática" equívocamente implementadas. Las fuentes de las empresas competidoras en muchos casos es gente inescrupulosa que pertenece a la misma empresa pero que se dedica al tráfico de información para sacar lucro (Posso y Lopez, 2012)

Es por ello que a esta investigación le anteceden políticas informáticas existentes en diferentes organizaciones en el mundo que se han revisado y analizado para mantener una idea clara de su estructura y operatividad; las empresas actualmente se enfocan solo en lo tecnológico, sin tomar en cuenta que la seguridad de la información es un problema que se debe mitigar y crear políticas y controles para formar ambientes seguros que garanticen y protejan la información para su buen uso y funcionamiento, esto conlleva a generar una serie de inconvenientes que no se puedan afrontar con tiempo y rapidez. (Guerrero y Suárez, 2016).

Visto de esta forma, este trabajo busca orientar y aportar con un plan de seguridad específicamente de bases de datos para los Gobiernos Autónomos Descentralizados, quienes han brindado la apertura para poder realizar esta tarea de investigación.

### **1.1. Problemática**

En los Gobiernos Autónomos descentralizados del Ecuador, normalmente existe una Unidad de Tecnologías encarga de tres áreas:

1. Software y Bases de Datos
2. Hardware – Infraestructura Tecnológica
3. Redes y Comunicaciones

La infraestructura de sistemas existente representa una inversión considerable en los activos de la organización, los lineamientos sobre el uso adecuado de los equipos de cómputo sugieren un tiempo de vida útil menor, haciendo que las reparaciones e inversión por actualización sean muy recurrentes.

Sin embargo no se han encontrado normativas establecidas que permitan mantener un esquema de trabajo seguro para la información, los servidores donde están alojadas las bases de datos son vulnerables, no se encuentran en un área donde el acceso restringido o pueda ser vigilado, trabajan los servidores en un ambiente inadecuado al no ser parte de un data center climatizado a al menos en 15 grados de enfriamiento, carecen de políticas de acceso y

operación de los servidores, así como también carecen de mecanismos de control en cuanto a la conectividad de la red que brinda en muchos casos acceso directo a las bases de datos.

Por los antecedentes mencionados y para lograr el éxito en el tema de seguridad, confidencialidad y protección de información, es de gran relevancia en la actualidad en las diferentes instituciones, que la información no este expuesta a ningún peligro o amenaza en caso de presentarse una contingencia pueda recuperarse en tiempo oportuno (Vásquez, 2017).

## **1.2. Justificación**

Tener un plan de seguridad es de gran beneficio para una organización, porque le permite establecer controles y políticas informáticas que serán un lineamiento para el buen uso del hardware, software, red e información que es generada y almacenada en los equipos de la institución.

Esta institución se beneficiaría y se ahorraría dinero y grandes pérdidas en su infraestructura de sistemas, los lineamientos estarían muy claros sobre el uso adecuado de los equipos de cómputo y su tiempo de vida útil se prolongaría, reduciendo la inversión en costosos mantenimientos externos. Vásquez (2017) Afirma que:

La principal debilidad que se presenta al momento de brindar el soporte necesario para superar algún percance, es la falta de conocimiento técnico y el uso de un método ágil que nos lleve a superar rápidamente los problemas, además de la falta de recursos y herramientas informáticas. (p. 2)

Sobre la base de las ideas expuestas es importante que antes de utilizar la tecnología, se tengan reglas y controles claros sobre el uso adecuado de equipo de cómputo, software, accesos a bases de datos y redes, esto incrementaría además la productividad de los usuarios. Con este Plan se beneficiará enormemente a las organizaciones que se sujeten de esta investigación, en cuanto se lograrán establecer lineamientos tecnológicos apegados a normas y estándares mundiales como la ISO 27002, donde se utilizaran los controles y se brindarán estrategias para definirlos como políticas institucionales.

## **1.3. Objetivo General**

Desarrollar un Plan de Seguridad de Base de datos para reducir la vulnerabilidad ante pérdidas de información en los Gobiernos Autónomos Descentralizados del Ecuador.

La forma de conseguirlo, establecidas como objetivos específicos son:

- Hacer un análisis situacional de la seguridad de la información en la organización investigada (presentado en este documento como estudio de caso).
- Determinar estándares relacionados a la seguridad de bases de datos y su entorno.
- Desarrollo Teórico de un Plan de Seguridad de Bases de Datos con sus componentes.

## **2. MARCO TEÓRICO**

### **2.1. La seguridad de la Información**

Comúnmente existen amenazas en las TIC's, las cuales se encuentran repartidas en diversos niveles de criticidad según sea la orientación y el ámbito de su utilización. En las empresas es muy alarmante el espionaje industrial, el robo de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

Pero es necesario enfatizar que diariamente, se realizan distintos métodos que perjudican a la seguridad de la información de las empresas, por lo tanto se hace necesario utilizar una estrategia completa de seguridad, de manera que se pueda prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas, que también son consideradas factores de riesgo, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

De esta manera no se pueden evadir los factores de riesgo por desastres ya que al no estar previstos de manera eficiente y sin planes de contingencia y/o de recuperación pueden causar

daños irreparables en tiempo y costos de recuperación, lo cual es muy difícil cuantificar, puede incluso determinar la continuidad de las operaciones en una organización. (Salazar, 2013)

Además la seguridad de la Información tiene como finalidad proteger tanto la información como los sistemas de la información del acceso, uso, divulgación, disrupción o destrucción no autorizada. Los términos Seguridad de Información, Seguridad informática y garantía de la información son utilizados con frecuencia y aunque su significado no es el mismo, tienen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información. Sin embargo, entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio (Guerrero & Suarez, 2016,p 18).

Ante todo la Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma que los datos puedan tener: electrónicos, impresos, audio u otras formas. Las instituciones gubernamentales, financieras, Hospitales y empresas privadas almacenan una gran cantidad de información confidencial ya sea de sus empleados, clientes, productos, situación financiera, etc. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en ordenadores y transmitida a través de las redes a otros ordenadores.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o la nueva línea de productos caigan en manos de un competidor o se vuelva pública en forma no autorizada, podría causar la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la empresa. Por lo tanto proteger la información confidencial es un requisito primordial, y en muchos casos también un imperativo ético y una obligación legal.

El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos. (Sánchez, 2010).

### **2.1.1. Objetivos de la seguridad de la información**

La seguridad de la información se encarga de protegerla, lo cual se conseguirá preservando la confidencialidad, integridad y disponibilidad de la información, como aspectos principales y el control y autenticidad como aspectos secundarios. A continuación se detallan varias características:

- La Integridad de la Información se refiere a la característica que hace que su contenido continúe inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. Una falla de integridad puede ser dada por diversas causas, entre ellas se encuentran: anomalías en el hardware, software, virus informáticos o ediciones por parte de personas que se infiltran en el sistema.
- La Disponibilidad u operatividad de la Información se refiere a su capacidad de estar en todo momento disponible para ser procesada por usuarios autorizados, para ello es necesario la información se mantenga almacenada de forma correcta, además de que el hardware y el software esté operando y que se respeten los formatos para su recuperación en forma satisfactoria.

- La Confidencialidad de la Información se refiere a la necesidad de que ésta sólo sea conocida por usuarios con autorización. Si ocurre falta de confidencialidad, la información puede provocar severos daños a su dueño.
- El Control sobre la información admite certificar que sólo los usuarios con autorización puedan decidir cuándo y cómo permitir que se acceda a la misma.
- La Autenticidad permite definir que la información requerida es válida y servible. Asimismo también permite afirmar el origen de la información, validando el emisor de la misma, para impedir sustitución de identidades.

### **2.1.2. Sistema de gestión de seguridad de la información**

Denominado SGSI, es un conjunto de procesos, políticas, y procedimientos organizados de manera lógica y soportada por objetivos a nivel estratégico de la empresa:

- Se puede organizar todas las medidas de seguridad basándose en los objetivos de la empresa y disminuir los riesgos, cambiando el escenario actual en el cual la seguridad es un gasto y transformándola en una herramienta para viabilizar empresas más seguras.
- Adquiere el ciclo de Deming (Planear-Hacer-Revisar-Actuar) para su gestión. Base de todas las normas ISO para mejora continua. (Chávez, 2013)

### **2.1.3. Vulnerabilidades en la seguridad de la información**

Las vulnerabilidades son aquellas debilidades internas de un sistema de Información las mismas que en caso de ser explotadas podrían causar un gran daño. La existencia de una vulnerabilidad no causa por sí misma un daño, es necesario que se presente una amenaza para detonarla.

Es una deficiencia en lo que se refiere al diseño, implementación, operación o los controles internos en un proceso, que podría utilizarse para vulnerar la seguridad de un sistema. Si una vulnerabilidad no tiene una amenaza, es posibles que no requiera la implantación de un control, pero aun así debe ser reconocida y monitoreada para cambiarla.

Los Sistemas de Información en general poseen vulnerabilidades. Se debe tener en cuenta que éstos son desarrollados, implementados y/u operados por personas, por ello la probabilidad de error está siempre presente. Hay casos en que el administrador o programador instalan maliciosamente una falla en un sistema para ser explotados después. Asimismo, gran parte de las vulnerabilidades surgen de factores tales como la complejidad, la ignorancia o el costo de los controles financieros.

El punto para la gestión de riesgos y las auditorías es la identificación y corrección de las debilidades antes de que puedan ser manipuladas, o por lo menos, para reducir el rango de aplicación de las amenazas que puedan valerse de ellas, hasta el punto de que ya no sean creíbles. (Journal, 2009)

### **2.1.4. Amenazas de fuga de información**

En el mundo digital, el riesgo de brechas de seguridad, fugas o pérdidas de información nunca ha sido mayor. No sólo se ha multiplicado el volumen de información en circulación sino también el número de vías en las que la información puede ser almacenada y transferida sin el consentimiento del propietario.

A pesar de la mayor concienciación sobre los riesgos y amenazas a la seguridad que afrontan las empresas a nivel mundial, las brechas de seguridad están creciendo y amenazando la solidez de las empresas y la privacidad de sus clientes.

Aun cuando los administradores de Tecnología de Información tienen a su disposición una gran cantidad de soluciones de seguridad, los cibercriminales siguen atacando sistemas y robando información importante, la misma que puede ser utilizada situaciones tales como: fraude con tarjetas de crédito, robo de identidad y otras actividades maliciosas. Las empresas de cada sector continúan informando de vulnerabilidades de seguridad y sin embargo, aún permiten la exposición de su información más sensible y confidencial. (Reed, 2008)

## **2.2. Normas conocidas de seguridad de la información**

En la forma en la que se trabaja actualmente inmerso en el mundo de la seguridad de la información y la seguridad informática, también crece la necesidad de transmitir la educación en estos temas, no obstante en espacios laborales o educativos no es tan sencillo como el compartir con un amigo y decirle qué antivirus emplear en su computador o que métodos debería utilizar para proteger su celular del robo de información. Por ello, es necesario buscar guías y libros que instruyen en temas de cómo afrontar la seguridad de forma responsable, procedimental y direccionada al cumplimiento de los estándares mínimos requeridos para la tecnología actual.

Por otro lado haciendo un breve definición de la norma se dice que, es un estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. (Carvajal, 2013)

A continuación se muestran diversos estándares internacionales, que actualmente son muy empleados para buscar la protección de la información, el mismo que es el activo más valioso de toda empresa, en el constante proceso de la consecución de protección a nivel de integridad, disponibilidad y confidencialidad.

### **2.2.1 ISO 27001**

Este es un estándar creado para la seguridad de la información denominado ISO/IEC 27001, adoptado por ISO, el mismo está creado en base a un estándar británico llamado BS 7799. Este estándar es certificable y fue publicado por primera vez en el año 2005. Arévalo, Bayona, & Rico (2015) Afirman que:

El éxito en la implantación de un SGSI desde cualquier perspectiva empresarial depende del compromiso y la mentalidad de cambio de los niveles ejecutivos y directivos en las organizaciones, por tanto, el alcance del sistema requiere de un nivel de concientización de las esferas estratégicas y tácticas de la estructura empresarial, de esta forma la capacitación se convierte en un medio de sensibilización que conduce a la interiorización y al compromiso de cambio como escenario de competitividad empresarial.(p.129,130)

También se establecen todos los requisitos para implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) a través del ciclo de Deming-PHVA mediante los procesos de planificar, hacer, verificar y actuar.

Cabe aclarar que el tema de certificación en aspectos de seguridad virtual, tal vez aún no ha sido considerado con la seriedad que merece en el ámbito empresarial. Cuando se analiza la norma ISO 27001, se nota que este estándar internacional ha sido desarrollado (por primera vez con relación a la seguridad) con toda la fuerza y detalle que hacía falta para empezar a presionar al ámbito empresarial sobre su aplicación. Es decir, se puede prever, que la certificación ISO-27001, será casi una obligación de cualquier empresa que desee competir en el mercado en el corto plazo, lo cual es lógico, pues si se desea interrelacionar sistemas de clientes, control de stock, facturación, pedidos, productos, etc. entre diferentes organizaciones, se deben exigir mutuamente niveles concretos y adecuados de seguridad informática, sino se abren brechas de seguridad entre sí. (Rodas, 2016, p.4)



Esquema ISO 27001  
Fuente: (Rodas, 2016)

### 2.2.2 ISO 27002

Es una guía que muestra buenas prácticas desde los objetivos de control hasta los controles recomendables a nivel de seguridad de la información. Se diferencia de la ISO 27001 ya que este no es un estándar certificable. Cuenta con 39 objetivos de control y 133 controles los mismos que están agrupados en 11 dominios, teniendo más controles y dominios que los creados en el estándar ISO 27001.

Con este documento se logra identificar un mayor marco de trabajo para una empresa cuando se desea implementar políticas de seguridad, fundar un sistema de gestión de la seguridad de la información y con la sensatez requerida para lograr la certificación ISO 27001 que evalúa menos dominios.

### 2.3. La base de datos empresarial

Desde la perspectiva más general durante el transcurso del tiempo las empresas se caracterizaron por el manejo de la creciente cantidad de información lo cual conlleva a utilizar diversas técnicas de almacenamiento de datos, siendo importante las bases de datos ya sea por la información almacenada o por el posible acceso rápido a ella. Las bases de datos crean un gran interés tanto por la atención que alcanza en los planes de estudio como por la habitual aparición en libros, proyectos, lo que nos hace indicar que es una técnica universal.

Las bases de datos, se usan habitualmente para el almacenamiento de información y que permita acceder rápidamente a la información, y además como soporte para la toma de decisiones. Por ello una ventaja importante es poder convertir los datos en información útil para la toma de decisiones, lo mismo que favorecerá a la dirección de la empresa en cuanto a su gestión empresarial. (Amado, 2014)

#### 2.3.1. Diseño de la Base de Datos

El crear una base de datos no es una tarea simple, esta tiene tres fases, las cuales son: conceptual, lógica y física. Asimismo es importante continuar con el orden de las fases ya que su labor es dificultosa pero también es importante que el diseñador de la base de datos entienda cuales son las necesidades de que tienen los usuarios.

Por tal motivo es importante comprender y recopilar toda la información proporcionada por el usuario y que se desee almacenar en la base de datos, por ende los diseñadores deberá interactuar con los usuarios. Cuando el diseñador comprenda la información con la que desea trabajar, se encontraría en la primera fase, en la que se conoce como diseño conceptual que radica en la creación de un esquema o modelo conceptual de la base de datos, el mismo que

es libre de los sistemas de gestión de base de datos o lenguajes de programación. Por lo tanto los usuarios que no son técnicos tienen que entender bien el funcionamiento. En el transcurso de esta fase, los diseñadores por lo general crean un diagrama con el objetivo de que les sirva como ayuda para visualizar la base de datos.

La segunda fase se la denominada diseño lógico que radica en modificar el esquema conceptual en un modelo de datos para un sistema de gestión de bases de datos determinado, el mismo que se trata de un esquema relacional. Representa como se estructuran los datos más cerca de la implementación.

En la última fase es el diseño físico, en la cual el diseñador se tiene que encargar de materializar el esquema relacional, es decir, mantener una coherencia entre el diseño anterior de la base de datos, tablas y restricciones de integridad. También tendrá que seleccionar métodos de acceso específico para los datos con la finalidad de conseguir buenas prestaciones y por otro lado diseñar las medidas de seguridad que requieran los datos. (Amado, 2014)

## **2.4. Buenas prácticas de seguridad con bases de datos**

Las bases de datos son con gran frecuencia el punto estratégico de los ataques de seguridad por los hacker's. Aquellas bases de datos que tienen información relacionada con la seguridad, las contraseñas y los datos financieros de los usuarios son de donde los atacantes buscan obtener mayores ganancias. Por tal motivo la seguridad de base de datos es un tema muy complejo que puede ser cubierto en detalle elaborado.

A continuación se detallan varias prácticas en seguridad de base de datos que ayudarán a las empresas:

- **Cifrado de archivos**

El hecho de almacenar la base de datos en un servidor independiente no razón suficiente para protegerse múltiples ataques. Cifrar todos los archivos que se guardan. Los archivos guardados del software web tienen la información que le permita conectarse a las bases de datos. Si se almacena la información en archivos de texto plano como por ejemplo una serie de usuarios, entonces se va a facilitar los datos que el hacker necesita para llegar a la información sensible.

No son sólo los archivos que necesitan ser encriptados. Sino también el cifrado de los archivos de copia de seguridad también en caso que haya un ataque interno.

- **WAF (Web Application Firewall's)**

Se recomienda utilizar un WAF, o un firewall para nuestras aplicaciones web, ya que hacen posible proteger el servidor ante ataques relacionados con el ingreso de secuencia de comandos, o de ataques específicos en el internet. Se recomienda integrar los 2 tipos de WAF uno en la red de la empresa, y otro en las aplicaciones o servidores web de la misma. Es importante entender que un ataque de inyección SQL, puede revelar información muy sensible, como usuarios y sus datos privados, y dicha información puede ser útil para el hacker ya que puede alterar nuestro sistema.

- **Actualización y Parches**

Esto es algo que muchos administradores web no saben manejar o controlar. Los sitios web que tienen una gran cantidad de aplicaciones de terceros, elementos, widgets, plugins y otros add, un tercero se convierten en blancos fáciles para algo que podría haber sido parcheado a tiempo.

- **Reducir el uso de aplicaciones de terceros**

Disminuir el número de aplicaciones de terceros que se utiliza. Tanto los widgets como otros contenidos se utilizan para mejorar la interfaz y hacer que luzca más atractiva, pero también crean vulnerabilidades. Por lo tanto es recomendable utilizar menos aplicaciones de terceros, ya que estos son hechos por programadores que después de un tiempo dejan de dar soporte y por ende el sistema puede quedar expuesto a ciertos ataques.



- **No compartir servidores**

Si la base de datos existente contiene información muy sensible, entonces se recomienda evitar usar un servidor compartido. Tiene la ventaja de ser más barato y más fácil, pero también hay que tener en cuenta que se está poniendo datos importantes y sensibles a manos de otra persona. En caso de no poder evitarlo, se recomienda hacer un scan o test profundo de todo su protocolo de seguridad.

- **Controles de seguridad**

Se recomienda activar todos los controles de seguridad de su base de datos. Asimismo revisar los filtros o controles de seguridades y asegurarse de que se han habilitado a pesar de que se activa automáticamente por la mayoría de las bases de datos en estos días.(Devpy, 2015)

#### **2.4.1. Importancia de la información empresarial**

Actualmente la información representa un recurso muy importante para una empresa, ya que gracias a ella, las empresas pueden mejorar y automatizar procesos operativos, asimismo admiten crear procesos para la toma de decisiones logrando ventajas competitivas e indica el rumbo que tomará la empresa, ya sea el caso del éxito o del fracaso. Tal información es muy vulnerable a ataques o amenazas internas y es susceptible a pérdida, deterioración o robo, ya que puede ser borrada, mal utilizada, sabotea o divulgada.

La información es el principal elemento a proteger, recuperar y resguardar dentro de las redes empresariales, esto genera una dependencia a los sistemas de información haciéndolas más vulnerables a las amenazas concernientes a la seguridad informática. El uso compartido de los recursos incrementa la dificultad de lograr el control a los accesos y la tendencia a los sistemas distribuidos ha debilitado la eficiencia del control técnico centralizado. (Rodas Mira, 2012 , p. 4)

Es muy difícil imaginarse una empresa que no contenga información que le permita desarrollar y detallar las actividades y estrategias que aplicará para competir en el mercado.

En ocasiones las empresas no logran recuperarse de estos daños relacionados con pérdida de información. Es indispensable para la operación de una empresa la protección de sus datos, principalmente en sus repositorios de información, como lo son sus bases de datos ya que son estas las que sustentan, aseguran y mantienen las características que la información debe tener para soportar un sistema de información auxiliado por computadora. (Molina, 2011)

#### **2.4.2 El Sistema de Gestión de la Continuidad del Negocio**

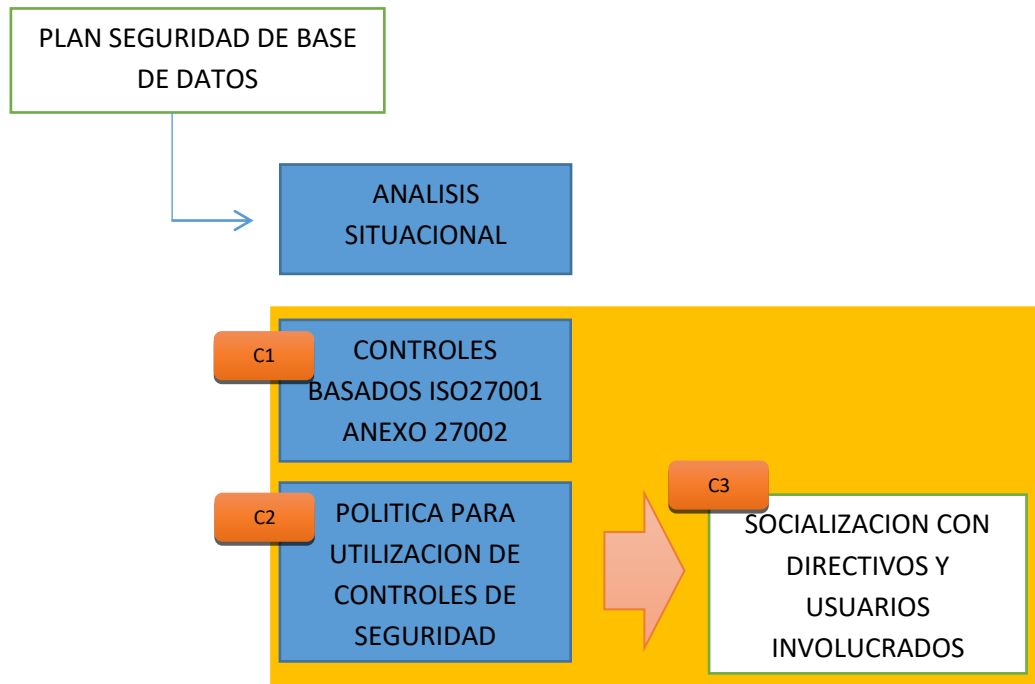
El Sistema de Gestión de la Continuidad del Negocio (SGCN) se ha convertido en una exigencia para las empresas que compiten el día de hoy en los mercados globalizados. La tendencia mundial es que ya las empresas no compitan entre sí: la competencia es entre cadenas de suministros. Una cadena de suministros, para mantenerse operando, no puede tener ningún eslabón débil; ninguno de sus componentes puede dejar de operar ya que si un elemento del todo dejara de funcionar se paraliza toda la serie, generando el caos. Cada miembro del sistema tiene que demostrar que es un proveedor confiable. Esto se logra teniendo en cada empresa un SGCN que proteja a los procesos esenciales que permiten originar los productos o servicios que desea el cliente. (Alexander, 2012, p. 2)

### **3. DESARROLLO DEL PLAN**

#### **3.1. Planteamiento del esquema general del plan**

Este plan estará conformado de componentes que permitirán desarrollarlo de forma consolidada, iniciando con un análisis situacional como medio de diagnóstico, que permite hacerle una radiografía para conocer de mejor forma a la organización; basado en este conocimiento se implementará un mecanismo de relacionan con los controles de la norma ISO 27001, anexo 27002, para luego proponer una política institucional de funcionamiento que permita reducir riesgos y vulnerabilidades de la base de datos; para finalizar este plan es importante socializarlo.

El objetivo principal consiste en el análisis de madurez de la organización que siendo de pequeño tamaño, para la implantación de la ISO/IEC 27001 se deben aplicar todas las fases del SGSI; no solo para conocer el estado actual en Seguridad de la Información, si no para que se puedan ajustar todos los elementos que se necesitan para poder acceder a mediano plazo a una certificación en la norma ISO / IEC 27001 versión 2013. (González, 2015, p. 4)



Esquema general del plan  
Fuente: Elaborado por los autores.

Cabe resaltar que cuando se inicia un proyecto de implantación del modelo de seguridad de la información en una empresa, se debe asignar a un responsable del proceso de documentar las cláusulas globales y luego las focales. La documentación es muy importante pues ésta controla por fechas las modificaciones y el estado de las revisiones; cuando aparece el término procedimiento documentado dentro del estándar, significa que el procedimiento debe ser establecido, documentado, implementado y mantenido. (López, 2013. P. 7)

### 3.2. Descripción de los componentes del plan

#### COMPONENTE 1

##### APLICACIÓN DE CONTROLES

**OBJ** : Objetivos de Control Norma ISO 27002

**DOM**: Dominio

**CTRL**: Controles

**-DOM** : Aspectos Organizativos de Seguridad de la Información

**OBJ: Organización Interna**

- **CTRL: Acuerdos de Confidencialidad**  
Es necesario siempre identificar y revisar de forma regular los acuerdos y aquellos requisitos de suma confidencialidad o no divulgación puedan contemplar las necesidades de protección de la información de la Organización. (ZohoWiki, 2015)
- **CTRL: Identificación de los riesgos derivados del acceso de terceros**  
Se deberían identificar riesgos a la información organizacional y a las instalaciones donde se procesa información de los procesos más importantes del negocio que impliquen a terceros y se deberían implementar además controles apropiados antes de conceder accesos. (ZohoWiki, 2015)
- **CTRL: Tratamiento de la seguridad en contratos con terceros**  
Los acuerdos realizados con terceras partes que impliquen el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes. (ZohoWiki, 2015)

## **DOM: CONTROLES DE ACCESO**

### **OBJ: Control de Acceso a la Red**

- **CTRL: Políticas de uso de los servicios en la Red**  
Se debería proveer políticas seguras a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados su utilización . (ZohoWiki, 2015)  
Es necesario que se realicen las conexiones a datos patrones mediante SSL 3.0/TLS 1.0 utilizando certificados ascendentes globales, estos certificaran que los usuarios realicen una conexión segura desde sus navegadores a los servicios.  
Asimismo se deben identificar sesiones de usuarios individuales que se vuelven a revisar con cada transacción usando aserciones de seguridad encriptadas XML mediante SAML 2.0.
- **CTRL: Autenticación de usuarios para conexiones externas**  
Es importante para proteger la Base de Datos utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios. (ZohoWiki, 2015)
- **CTRL: Identificación de los equipos en las redes**  
Es necesario utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios. (ZohoWiki, 2015)  
  
Se debe enrolar cada equipo a usar en red en la institución
- **CTRL: Protección de los puertos de diagnóstico y configuración remotos**  
Se deberá controlar la configuración y la forma de acceso físico y lógico a los puertos de diagnóstico. (ZohoWiki, 2015)
- **CTRL: Segregación de las redes**  
Se deberían segregar los grupos de usuarios, servicios y sistemas de información en las redes. (ZohoWiki, 2015)  
Para diferenciar y permitir acceso a la Base de Datos, solamente a los que cuentan con roles implícitos a su utilización.
- **CTRL: Conexión a la Red**  
En cuanto a toda la red compartida, especialmente la que se extiende más allá de los límites de la propia Organización, se deberá restringir las competencias

de los usuarios para conectarse a la red según la política de control de accesos y necesidad de uso de las aplicaciones de negocio. (ZohoWiki, 2015)

**OBJ: Control de Acceso al Sistema Operativo**

- **CTRL: Desconexión automática de sesión.**  
Se deberían desconectar las sesiones tras un determinado periodo de inactividad. (ZohoWiki, 2015)

**OBJ: Control de Acceso a las aplicaciones y a la información**

- **CTRL: Restricción del acceso a la Información**  
Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida. (ZohoWiki, 2015)

**OBJ: Seguridad de los archivos de sistemas**

- **CTRL: Protección de los datos de prueba del sistema**  
Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas. (ZohoWiki, 2015)
- **CTRL: Control de acceso al código fuente de los programas**  
Se debería restringir el acceso al código fuente de los programas. (ZohoWiki, 2015), especialmente de los que tienen acceso a la base de datos.

**OBJ: Seguridad en los procesos de desarrollo y soporte**

- **CTRL: Procedimiento de control de cambios.**  
Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios. (ZohoWiki, 2015), especialmente de los que tienen acceso a la base de datos y su estructura.
- **CTRL: Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.**  
Se deberían revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización. (ZohoWiki, 2015), especialmente de los que tienen acceso a la base de datos.
- **CTRL: Restricciones a los cambios en los paquetes de software**  
Se debería desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados. (ZohoWiki, 2015)
- **CTRL: Externalización del desarrollo del software**  
Se debería supervisar y monitorizar el desarrollo del software subcontratado por la Organización. (ZohoWiki, 2015), brindando acceso cuando es relacionado a la base de datos, solamente a una base de datos con estructura lógica parecida a la original.

**DOM: GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

**OBJ: Aspectos generales de la seguridad de la información**

- **CTRL: Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información**  
Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requerido, tras la interrupción o fallo de los procesos críticos de negocio. (ZohoWiki, 2015)

## **DOM: GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

### **OBJ: Aspectos generales de la seguridad de la información**

- **CTRL: Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información**

Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempos requeridos, tras la interrupción o fallo de los procesos críticos de negocio. (ZohoWiki, 2015)

## **DOM: CUMPLIMIENTO**

### **OBJ: Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico**

- **CTRL: Cumplimiento de las políticas y normas de seguridad**

Los directivos se deberían asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad. (ZohoWiki, 2015)

## **DOM: SEGURIDAD FISICA Y DEL ENTORNO**

### **OBJ: Controles físicos y ambientales**

- **CTRL: Perímetro de seguridad física (AREAS SEGURAS)**

Seguridad mediante personal durante las 24 horas.

Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. (ZohoWiki, 2015)

- **CTRL: Controles físicos de entrada (Acceso restringido a través de tarjetas de proximidad)**

Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. (ZohoWiki, 2015)

### **OBJ: SEGURIDAD DE LOS EQUIPOS**

- **CTRL: Instalación y protección de equipos (Equipo informático en áreas de acceso controlado / Vigilancia con video en toda la instalación y el perímetro)**

El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. (ZohoWiki, 2015)

Sensores de detección de humo e incendio en todos los centros de datos, con sistemas ECARO 25

Los centros de datos también están protegidos con sistemas de rociadores de tubería húmeda

Hay extinguidores de incendio en todas las instalaciones

- **CTRL: Suministro Eléctrico Alimentación eléctrica subterránea / Sistemas de alimentación ininterrumpida (UPS), Unidades de distribución de energía (PDU) redundantes, Generadores diésel con almacenamiento de combustible diésel en el lugar)**

Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo. (ZohoWiki, 2015)

- **CTRL: Seguridad del cableado**

Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños. (ZohoWiki, 2015)

- **CTRL: Seguridad en la reutilización o eliminación de equipos**

Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación.

Estos pueden brindar nuevamente acceso a la Base de datos y vulnerarla

- Control de humedad y temperatura
- Suelo elevado para facilitar la circulación continua de aire

## **DOM: CONTROLES DE ACCESO**

### **OBJ: REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO**

- **CTRL: Política de control de accesos**

Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización. (ZohoWiki, 2015)

- **CTRL: Registro de usuarios y Gestión de privilegios**

Se debería restringir y controlar la asignación y uso de los privilegios. (ZohoWiki, 2015)

- **CTRL: Gestión de contraseñas de usuario**

Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal. (ZohoWiki, 2015)

## **COMPONENTE 2**

### **ELABORACION DE POLITICAS INSTITUCIONALES**

En este plan se incorporaran controles importantes que provienen de la revisión de la norma iso27001 y su anexo 27002; es necesario que se adopten como políticas institucionales, siendo aprobadas por la máxima autoridad de la organización.

Es importante fundamentarse además en la norma de control interno de contraloría, en su numeral: “410-04 Políticas y procedimientos”, donde se menciona que “la máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria” (NCI de contraloría, 2012).

Es decir en la política incorporar los controles normalizados en la ISO 27001, como medida de reducción de las vulnerabilidades, dependiendo del dimensionamiento de la organización.

## **COMPONENTE 3**

### **SOCIALIZACION DEL PLAN**

Al finalizar el Plan de seguridad, es decir, una vez que ya está aprobado, es necesario que se realice una socialización, donde como estrategia se podrán elaborar talleres donde se expondrá de forma clara cuál es el beneficio de utilizar controles y asegurar la base de datos, así mismo se explicará situaciones de riesgo que se tendría que mitigar.

Una de las razones claves por las cuales se debe socializar un plan de seguridad, es que al hacer participar al usuario se reduce el riesgo en gran medida, ya que se tiene informado a los usuarios de posibles soluciones de peligro y vulnerabilidad en cuanto a pérdida de información.

## CONCLUSION

Luego de haber realizado y revisado metodologías y estándares de análisis de riesgos se puede concluir que existen herramientas y se encuentran disponibles para la realización de un buen análisis de riesgos; estas herramientas no solamente suelen ser software o equipos de alta complejidad; también existen documentos guía que facilitan la detección de riesgos, pudiendo resultar más óptimo delegar este tipo de tareas a alguna empresa consultora externa.

Se han realizado investigaciones en ocho Gobiernos Autónomos Descentralizados dentro de la provincia de Los Ríos y Bolívar, para el desarrollo de la presente metodología del plan se realizó un breve análisis de riesgos, identificando los activos (datos, hardware, software, servicios, personal) con mayor riesgo, amenazas y vulnerabilidades que pueden permitir acceso libre a las bases de datos; se realizó una visión generalizada de cómo se encuentran expuestas las bases de datos en función de la probabilidad de que una amenaza ocurra.

Seleccionar de forma correcta los controles para el tratamiento del riesgo y amenazas permite evaluar la estrategia o acción más apropiada para tratar de que no ocurran inconvenientes, estos controles deben ser los adecuados para disminuir las vulnerabilidades.

Es muy probable que en los Gobiernos Autónomos Descentralizados se presenten situaciones donde no se puedan determinar controles ni tampoco pueda ser viable diseñarlos sin embargo aplicando políticas claras se podría lograr reducir el riesgo.

Se concluye además que se considera necesario evitar el riesgo, no debiendo ser una opción; cualquier acción donde las actividades y sub sistemas de la organización, o las maneras gestionar el negocio, se modifican pueden lograr también evitar la ocurrencia del riesgo.

El documento Plan de Seguridad que se plantea, muestra la selección de los controles aplicables a la base de datos, que partió de hacer un análisis situacional de la seguridad de la información en la organización investigada, además se establecieron controles del entorno a la Base de Datos.

Esta investigación está limitada a la descripción de controles y para su incorporación y aplicación en una política informática institucional, no se han utilizado únicamente el estándar ISO 27001 con su anexo 27002; por lo que se propone a la organización sujeta de esta investigación, los siguientes trabajos futuros.

## BIBLIOGRAFIA:

- Posso Guerrero , R. E., & López, P. (2012). *Desarrollo De Políticas De Seguridad Informática E Implementación De*. Ingeniería en Electrónica y Telecomunicaciones.
- Vasquez Naranjo, W. M. (2017). *Propuesta De Un Método Para Elaborar Un Plan De Recuperación De Desastres (Drp) En El Área De Tecnología De La Información Para Cooperativas Del Ecuador*. Escuela Superior Politécnica De Chimborazo.
- Amado, R. B. (2014). *Bases de datos y minería de datos en contornos empresariales*. Obtenido de [http://ruc.udc.es/bitstream/2183/12431/2/BlancoAmado\\_RosanaMaria\\_TFG\\_2014.pdf](http://ruc.udc.es/bitstream/2183/12431/2/BlancoAmado_RosanaMaria_TFG_2014.pdf)
- Chávez, R. (2013). *Gestión de riesgos de seguridad de la información*. Obtenido de <http://es.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin>
- Devpy. (2015). *Seguridad y Bases de Datos*. Obtenido de <http://365bytes.com/2015/01/25/seguridad-y-base-de-datos-buenas-practicas/>
- Journal, I. (2009). *Vulnerabilidades sistemas de información*. Obtenido de <http://www.bscconsultores.cl/descargas/B.2%20Vulnerabilidad.pdf>
- Molina, S. L. (2011). *Prácticas a seguir para proteger la información*.
- Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). *Implantación de un sistema de gestión de seguridad de información. Universidad Distrital Jose Francisco de Caldas*.

- Reed, S. (2008). *Riesgos y amenazas de la fuga de información en las empresas*. Obtenido de <http://www.revistadintel.es/Revista1/DocsNum20/PersEmpresarial/Reed.pdf>
- Salazar, J. B. (2013). *Modelo para seguridad de la Información TIC*. Obtenido de <http://ceur-ws.org/Vol-488/paper13.pdf>
- Sanabria, J. B. (2011). *Buenas Practicas, estándares y normas TI*. Obtenido de <http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas>
- Sánchez, E. G. (2010). *Calidad y seguridad de la información y auditoría informática*. Obtenido de <http://e-archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf?sequence=1>
- Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información. *Universidad Distrital Jose Francisco de Caldas*.
- González Martínez, J. (2015). Elaboración de un Plan de implementación de. *Universitat Oberta de Catalunya*.
- Guerrero Melo, J., & Suarez Catrellon, F. J. (2016). Planeacion Del Sistema De Gestión De Seguriad De La Informacion Aplicando La Norma Internacional Iso/lec 27001:2013 En Área Contable En La Empresa Transformadores Cdm. *Universidad Francisco De Paula Santander Ocaña*.
- Alberto G. Alexander. (2012). *Nuevo Estándar Internacional En Continuidad Del Negocio Iso 22301:2012*
- Rodas Mira, A. (s,f). Analisis y Especificacion de Requerimientos de Seguridad Informatica en las Empresas. *Universidad San Buena Ventura Medellin, Colombia*.
- Lopez Castaño, L. A. (2013). *Sistema De Gestion De Seguridad De La Informacion En El Club Militar Desde La Norma ISO 27001:2005*
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Autenticación de usuario para conexiones externas*. Obtenido de <https://iso27002.wiki.zoho.com/11-4-2-Autenticaci%C3%B3n-de-usuario-para-conexiones-externas.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Gestión de privilegios*. Obtenido de <https://iso27002.wiki.zoho.com/11-2-2-Gesti%C3%B3n-de-privilegios.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Tratamiento de la seguridad en contratos con terceros*. Obtenido de <https://iso27002.wiki.zoho.com/6-2-3-Tratamiento-de-la-seguridad-en-contratos-con-terceros.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001*. Obtenido de <https://iso27002.wiki.zoho.com/6-1-5-Acuerdos-de-Confidencialidad.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001*. Obtenido de <https://iso27002.wiki.zoho.com/6-2-1-Identificaci%C3%B3n-de-los-riesgos-derivados-del-acceso-de-terceros.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Autenticación de usuario para conexiones externas*. Obtenido de <https://iso27002.wiki.zoho.com/11-4-2-Autenticaci%C3%B3n-de-usuario-para-conexiones-externas.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Conformidad con la política de seguridad*. Obtenido de <https://iso27002.wiki.zoho.com/15-2-1-Conformidad-con-la-pol%C3%ADtica-de-seguridad.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Control de acceso a la librería de programas fuente*. Obtenido de <https://iso27002.wiki.zoho.com/12-4-3-Control-de-acceso-a-la-librer%C3%ADa-de-programas-fuente.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Control de conexión a las redes*. Obtenido de <https://iso27002.wiki.zoho.com/11-4-6-Control-de-conexi%C3%B3n-a-las-redes.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Controles físicos de entrada*. Obtenido de <https://iso27002.wiki.zoho.com/9-1-2-Controles-f%C3%ADsicos-de-entrada.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Desarrollo externalizado del software*. Obtenido de <https://iso27002.wiki.zoho.com/12-5-5-Desarrollo-externalizado-del-software.html>
- ZohoWiki. (2015). *El Anexo de ISO 27001 - Desconexión automática de terminales*. Obtenido de <https://iso27002.wiki.zoho.com/11-5-5-Desconexi%C3%B3n-autom%C3%A1tica-de-terminales.html>



ZohoWiki. (2015). *El Anexo de ISO 27001 - Gestión de contraseñas de usuario*. Obtenido de <https://iso27002.wiki.zoho.com/11-2-3-Gesti%C3%B3n-de-contrase%C3%B1as-de-usuario.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Instalación y protección de equipos*. Obtenido de <https://iso27002.wiki.zoho.com/9-2-1-Instalaci%C3%B3n-y-protecci%C3%B3n-de-equipos.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Perímetro de seguridad física*. Obtenido de <https://iso27002.wiki.zoho.com/9-1-1-Per%C3%ADmetro-de-seguridad-f%C3%ADsica.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Política de control de accesos*. Obtenido de <https://iso27002.wiki.zoho.com/11-1-1-Pol%C3%ADtica-de-control-de-accesos.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Política de uso de los servicios de red*. Obtenido de <https://iso27002.wiki.zoho.com/11-4-1-Pol%C3%ADtica-de-uso-de-los-servicios-de-red.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Procedimientos de control de cambios*. Obtenido de <https://iso27002.wiki.zoho.com/12-5-1-Procedimientos-de-control-de-cambios.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Protección a puertos de diagnóstico remoto*. Obtenido de <https://iso27002.wiki.zoho.com/11-4-4-Protecci%C3%B3n-a-puertos-de-diagn%C3%B3stico-remoto.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Protección de los datos de prueba del sistema*. Obtenido de <https://iso27002.wiki.zoho.com/12-4-2-Protecci%C3%B3n-de-los-datos-de-prueba-del-sistema.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Redacción e implantación de planes de continuidad*. Obtenido de <https://iso27002.wiki.zoho.com/14-1-3-Redacci%C3%B3n-e-implantaci%C3%B3n-de-planes-de-continuidad.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Redacción e implantación de planes de continuidad*. Obtenido de <https://iso27002.wiki.zoho.com/14-1-3-Redacci%C3%B3n-e-implantaci%C3%B3n-de-planes-de-continuidad.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Restricción de acceso a la información*. Obtenido de <https://iso27002.wiki.zoho.com/11-6-1-Restricci%C3%B3n-de-acceso-a-la-informaci%C3%B3n.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Restricciones en los cambios a los paquetes de software*. Obtenido de <http://iso27002.wiki.zoho.com/12-5-3-Restricciones-en-los-cambios-a-los-paquetes-de-software.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Revisión técnica de los cambios en el sistema operativo*. Obtenido de <https://iso27002.wiki.zoho.com/12-5-2-Revisi%C3%B3n-t%C3%A9cnica-de-los-cambios-en-el-sistema-operativo.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Segregación en las redes*. Obtenido de <https://iso27002.wiki.zoho.com/11-4-5-Segregaci%C3%B3n-en-las-redes.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Seguridad del cableado*. Obtenido de <https://iso27002.wiki.zoho.com/9-2-3-Seguridad-del-cableado.html>

ZohoWiki. (2015). *El Anexo de ISO 27001 - Suministro eléctrico*. Obtenido de <https://iso27002.wiki.zoho.com/9-2-2-Suministro-el%C3%A9ctrico.html>