Controles de Seguridad Internos para implementar en SAP Business One.

Jesús Leonardo Perea Alarcón
Universidad Piloto de Colombia
Especialización en Seguridad Informática
Jesusp2104@gmail.com

Resumen
La implementación de controles internos en una empresa que utilice SAP Business One le permiten realizar una gestión de riesgos básica, disminuyendo su probabilidad e impacto. En este articulo se dan algunos controles fáciles de incorporar dentro de cualquier empresa, incluso sino cuenta con un departamento de tecnología, con el objetivo de asegurar las principales características de la información.

Abstract
The implementation of internal control in a company using SAP Business One lets you perform basic risk management, reducing their likelihood and impact. In this articule some easy controls to incorpórate within any given company, but even has a technology department in order to ensure the main features of information.

Palabras Clave: Riesgos, Controles, ERP, Empresa, Impacto.

Introducción

Un gran número de pequeñas y medianas empresas (PYMEs) están adoptando SAP Business One como su ERP principal, muchas de ellas utilizando SAP Business One como su primer sistema de gestión y otras reemplazando el actual o integrándolo con desarrollos in House. En cualquier caso, la adquisición de un ERP es una inversión significativa para una PYME y en este se depositan no solo gran parte de las esperanzas de la empresa para mejorar sus procesos y ser más productiva, también almacenan allí absolutamente toda la información de la empresa.

Es ahí donde SAP Business One se convierte en una herramienta vital para toda la compañía y sus funcionarios, que empiezan a ingresar, modificar y consultar información día a día. Este flujo de información lleva a las empresas a darse cuenta que el sistema empieza a demandar ciertas medidas a nivel de seguridad de la información que no se habían contemplado en principio y que para muchas son un mundo completamente desconocido que no saben cómo implementar.

Las empresas que adquieren el sistema no cuentan con una gran infraestructura, es importante indicar que muchas tienen áreas de tecnología no muy robustas que se encargan de las labores del día a día, otras subcontratan los servicios de tecnología en donde la mayoría de veces solo se encargan del soporte técnico y en la mayoría no se aplica ninguno de los dos casos anteriores y las labores referentes a tecnología se cargan a personas de confianza y/o personas que cuentan con algún conocimiento sobre el tema. Lo anterior no afecta la operación de las empresas en su día a día ya que los problemas que surgen van siendo subsanados o se transfieren a terceros para que se encarguen de dar una solución; sin embargo cuando una empresa adquiere un sistema como SAP Business One estas soluciones a las que vienen acostumbrados empiezan a no ser suficientes para soportar los requerimientos de seguridad que demanda el sistema.

En uno de los estudios realizados sobre incidentes de seguridad a nivel mundial [1] se encuentra información sobre ataques internos y externos en la cual indican que el porcentaje de ataques externos es mucho más alto que los internos, como puede verse en la figura 1, los ataques internos no alcanzan un 20% en el año 2013, mientras que los externos superan el 75% para el mismo año. Aunque esta información contrasta con un estudio realizado por ESET [2] en empresas de Latinoamérica donde se encuentran resultado que indican que solo la política de seguridad supera el 50% en cuanto a prácticas de gestión realizadas por las empresas, seguida de la auditoría interna con un 42%. Como dato importante se puede interpretar que el 7,3% de las empresas no implementan ninguna práctica de gestión, esto no es un dato menor ya que estamos hablando de casi 245 empresas de 3369 consultadas.

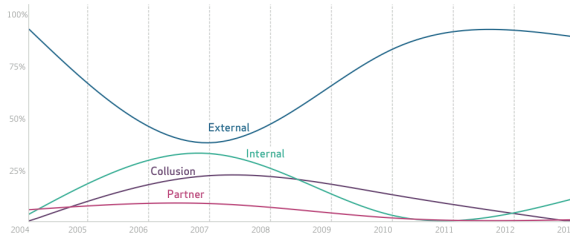

Fig. 1: [1] Percent of breach per threat actor category over time

1. Gestión de la Seguridad de la Información para SAP Business One

Las empresas confían en los Partner encargados para la implementación del sistema y todas las recomendaciones que estos realizan son realizadas sin objeción alguna, sin embargo, la idea principal del Partner es la productividad y las recomendaciones que este brinda son enfocadas a que el sistema sea más productivo, lo cual no es malo, simplemente es la idea principal del sistema, el problema aparece cuando un proceso es productivo pero es un riesgo potencial para la información de la empresa. La mayoría de las recomendaciones que realiza el Partner a nivel de seguridad de la información se enfocan a dos factores: 1) Uso del módulo de seguridad de SAP Business One. 2) Acceso remoto al servidor donde se encuentra SAP Business One.

El primer factor no es más que un módulo de gestión de claves que trae el sistema, donde se puede definir la complejidad de la clave (ver figura 2). Este módulo se aborda mas adelante con mayor profundidad.

El segundo factor son recomendaciones a las empresas para que las conexiones remotas se realicen de manera que los usuarios no se vean afectados, de manera que establezcan un control de acceso como es una VPN, pero que los usuarios se conecten por Escritorio remoto al servidor y allí ejecuten el cliente, esto se hace para ser más productivos. Otras recomendaciones sobre el acceso pueden ir dirigidas a establecer reglas o bloqueos en el Firewall y evitar ataques de Denegación de Servicio.

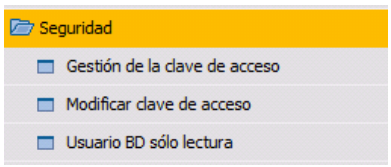

Fig. 2: [5] Módulo Seguridad SAP Business One

Este tipo de recomendaciones inducen a la empresa a pensar que los ataques a la seguridad de la información pueden ser originados exclusivamente por amenazas externas y enfocan sus esfuerzos en protegerse de dichos ataques, en la medida que les es posible. Esto ocasiona que muchas veces ni siquiera contemplan que los ataques pueden tener un origen desde el interior de la organización.

La idea que se plantea en este artículo no es la de desvirtuar o menospreciar la seguridad perimetral que las empresas puedan establecer, la idea es brindar información suficiente a las empresas para que realicen una debida gestión de la seguridad a partir de la implementación de controles desde el interior de la organización, de manera que la seguridad perimetral sea el control final dentro de la estructura de la gestión de la seguridad de la información, considerando que la mayoría de las PYMEs no cuenta con un área de tecnología definida existen varias recomendaciones que se pueden implementar desde otras áreas, en otros casos la empresa si debe considerar el acompañamiento de profesionales en tecnología, ya sea como outsorcing o contratados directamente. A continuación se enumeran las medidas más importantes que se deben establecer al interior de la empresa para el sistema SAP Business One.

La necesidad de gestionar la seguridad de la información parte del hecho de aceptar que toda empresa es propensa a la materialización de nuevos riesgos al implementar un sistema ERP. Las recomendaciones realizadas se han establecido tomando como guía la publicación especial de la NIST 800-30 [3] sobre la gestión de riesgos de sistemas informáticos y el ciclo de vida de desarrollo de un sistema, enfocándolos a la implementación y operación del sistema SAP Business One y abarcando aspectos muy generales que puedes ser aplicados por las empresas sin diferenciar su actividad económica o estructura organizacional.

Algunos de los riesgos que se pretenden mitigar con la adopción de las recomendaciones realizadas, son los siguientes:

- Accesos lógicos no autorizados a información confidencial de la empresa.
- Accesos físicos no autorizados al servidor que contiene la base de datos.
- Modificación de información confidencial de la empresa.

- Modificación de información contable y/o financiera de la empresa.
- Indisponibilidad de acceso a la información registrada en el sistema.
- Daño de la base de datos del sistema.

2. Gestión desde la Instalación

Dentro del ciclo de vida del sistema en la organización vamos a tomar la instalación como la fase inicial del ciclo. La gestión de la seguridad de la información para SAP Business One empieza antes de su implementación, incluso antes de su instalación. El período de implementación del sistema es un espacio de tiempo que, dependiendo del tamaño de la empresa y de la cantidad de procesos, puede demorar entre 2 o 6 meses en promedio y comienza con la instalación del sistema en el servidor, previamente se debe tener instalado un motor de bases de datos, el motor más utilizado para SAP Business One es SQL Server en las versiones desde 2005 hasta 2012.

Durante este período de tiempo la empresa le da acceso total al Partner a toda su infraestructura tecnológica, brindando usuario administrador del servidor, del motor de la base de datos, de los equipos clientes. La mayoría de veces la entrega de estos datos se realiza sin ningún tipo de medida de seguridad, se envía por correo electrónico en texto claro, se indican en actas de reuniones que son revisadas por varias personas o simplemente se divulgan verbalmente en presencia de usuarios. Las empresas deben realizar la entrega de usuarios con perfiles de tipo administrador solo en los casos que sean completamente necesarios y la entrega se debe realizar mediante actas que sean debidamente protegidas por parte del Partner y a las que solo tenga acceso el o las personas responsables de la parte técnica o por algún medio de comunicación electrónica que maneje algún tipo de cifrado para que la información no se vea comprometida en caso de ser interceptada.

Antes de entregar esta información es importante tener un acuerdo de confidencialidad firmado entre la empresa y el Partner, donde se indique la importancia de la información que se va a compartir y la vigencia de dicho acuerdo. Al terminar el período de implementación las claves que fueron indicadas al Partner deben ser modificadas.

3. Definición de roles y responsabilidades

SAP Business One provee a la empresa de un módulo donde según se pueden brindar permisos específicos para cada usuario, pero además de eso el modelo de licenciamiento es el primer filtro para la definición de cada usuario. Para entender mejor el tema el sistema cuanta con diferentes tipos de licencias, cada tipo de licencia tiene unos permisos ya definidos que no se pueden modificar, los tipos de licencias del sistema son:

1. Profesional
2. Limited CRM
3. Limited Logistics
4. Limited Financials
5. B1 Starter
6. CRM Sales

Por ejemplo la licencia Profesional puede crear Facturas, pero la licencia Limited CRM solo puede consultarlas, sin embargo, esta misma licencia Limited CRM puede crear Pedidos de Cliente y la Limited Financials solo puede consultar Pedidos de Cliente y Facturas. Estos permisos no se pueden modificar ya que son propios de la licencia y cada usuario solo puede tener una licencia asignada.

Partiendo de este punto la empresa debe establecer que rol dentro de la organización va a tener permiso para realizar documentos en el sistemas y cuales documentos, esta labor debe ir muy de la mano con la información de permisos que tiene cada licencia y el proceso que se establezca dentro de la empresa para ingresar la información al sistema. Esta actividad puede incluso ayudar a la empresa a disminuir costos de licenciamiento, ya que cada licencia tiene un costo diferente, siendo la licencia profesional la más costosa y la que muchas empresas seleccionan para la mayoría de usuarios cuando en términos de procesos y de seguridad no deberían tener acceso a todos los módulos.

Cada una de las definiciones que realice la empresa en cuanto a los roles y las licencias que le corresponden a cada uno debe ser documentado apropiadamente. En caso de que apliquen autorizaciones adicionales a las que vienen por defecto con la licencia se pueden establecer en el módulo de Autorizaciones del sistema como se puede ver en la Figura 3 en el módulo podemos especificar que permiso puede tener el usuario para un documento en específico. Estas autorizaciones que son adicionales también deben quedar documentadas.

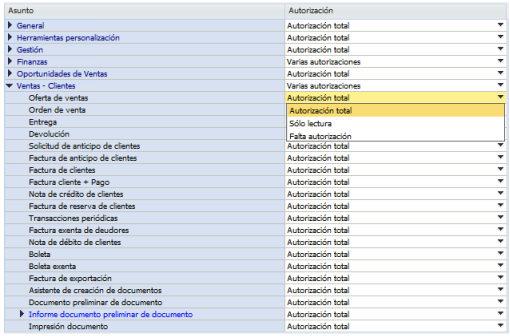

Fig. 3: [5] Opciones módulo Autorizaciones

3.1 Asignación de usuarios

Lo primero que se debe considerar aquí es ¿ quién realmente necesita usuario para ingresar al sistema?, para responder a este pregunta es imprescindible que la definición de las roles y responsabilidades planteadas en el punto anterior este muy aterrizado, es común que las empresas asignen usuarios a todos los funcionarios y cuando se realiza una auditoría se evidencia que algunos de los funcionarios no usan el sistema o ingresan esporádicamente a realizar actividades que se pueden encargar a usuarios concurrentes del sistema. Una vez definido que funcionarios requieren usuario y teniendo establecidos previamente los permisos del mismo, la recomendación para la asignación de los usuarios es que el nombre de usuario se pueda identificar fácilmente y se pueda relacionar con el funcionario. Así mismo que manejen una estructura definida y escalable, sin embargo, aquí nos encontramos con un inconveniente propio del sistema y es que la longitud máxima para el nombre del usuario es de 8 caracteres, lo que evita que se establezca como estructura nombre.apellido, de manera que una de las recomendaciones para la creación de los usuarios es colocar la inicial del primer nombre y el apellido. Un ejemplo de lo indicado es:
Juan Perez, usuario: jperez
En algunos casos se pueden utilizar las iniciales de los dos nombre y el primer apellido:
Juan Fernando Perez, usuario: jfperez

Lo que no es recomendable es utilizar el mismo usuario por cargo y dejar el usuario cuando exista una rotación de personal. Esto se puede dar para problemas en cuanto a la gestión de los usuarios y en caso de presentarse un incidente con ese usuario será difícil establecer quien lo estaba usando en determinado momento.

Cada asignación de usuarios debe realizarse formalmente y en lo posible con un acta de entrega donde se indique la responsabilidad del funcionario con el usuario asignado, del mismo modo, cuando el funcionario entregue el usuario debe realizarse un acta de entrega del mismo y se debe pasar la novedad a la persona encargada de realizar la des habilitación del usuario.

3.2 Complejidad para claves de acceso

El sistema en su módulo de seguridad incluye la opción de Gestión de la clave de acceso, aquí el sistema permite establecer la complejidad para las contraseñas con 4 niveles de seguridad: bajo, medio, alto, definido por el usuario. La recomendación en este punto es la de establecer un nivel alto. Como se puede ver en la figura 4, el nivel alto establece criterios como: vencimiento después de 30 días, longitud mínima de 8 caracteres, mínimo un carácter en mayúscula, mínimo un carácter en minúscula, mínimo un carácter no alfanumérico, histórico de 5 claves y 3 intentos fallidos antes de bloquear el usuario. Con el nivel de seguridad definido por el usuario se pueden personalizar estas opciones, pero la idea seria no disminuir las que este nivel ya tiene establecidas, a menos que una política general de la empresa tenga una definición de complejidad que implique realizar algún cambio. Es importante que las empresas no contemplen como opción dejar el nivel bajo ya que las contraseñas que se permiten en este nivel son muy débiles y no tienen vencimiento establecido.

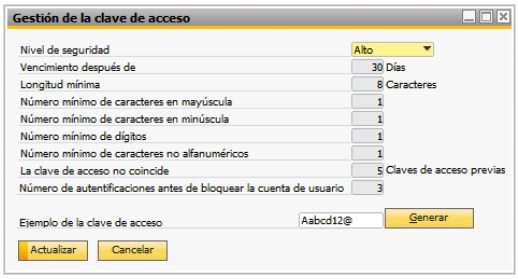

Fig. 4 : [5] Módulo de Gestión de la clave de acceso

4. Gestión de seguridad Motor de Bases de Datos

Hasta este momento las recomendaciones realizadas se han basado en establecer, implementar y documentar procesos que no necesariamente deben ser realizados por profesionales de tecnología, sin embargo, entendiendo la lógica del funcionamiento del sistema es esencial que se establezcan controles sobre el motor de base de datos, SAP Business One almacena toda su información en la base de datos haciendo de esta misma un activo critico para la empresa. La gran mayoría de

implementaciones de SAP Business One se realizan sobre el motor SQL Server de Microsoft.

A nivel de motor de base de datos los controles iniciales que se deben establecer vienen ligados a la instalación de SAP Business One, la cual requiere un usuario de SQL para establecer la conexión con la base de datos durante la instalación tanto del server como del cliente. En la gran mayoría de ocasiones se utiliza el usuario súper administrador (sa) para realizar todas las instalaciones, pero lo más recomendable es crear un usuario especifico para las conexiones que se establezcan con el sistema. Para la creación del usuario es necesario tener en cuenta que dicho usuario debe tener acceso a la base de datos que crea el sistema la cual se llama SBO-COMMON. La asignación de los roles para el usuario se deben basar en líneas base o guías de buenas prácticas específicas para el motor de base de datos que se utilice, para el caso de SQL Server si al usuario creado para toda la gestión del sistema se le asigna el rol sysadmin para evitar problemas durante la instalación, es importante retirar este rol posteriormente.

No solo a nivel de acceso podemos establecer controles, siendo la base de datos el activo más importante del sistemas es completamente necesario establecer un plan de backup de la base de datos. Para este plan de backup se puede utilizar el SQL Server Agent, que permite programar este tipo de tareas, sin embargo, también se puede optar por una acción manual o utilizar cualquier otra herramienta. Debe ser claro para la empresa que las copias de seguridad se deben almacenar en un disco de almacenamiento diferente al que utiliza el servidor, incluso utilizar un disco de almacenamiento extraíble o portable es una buena opción, siempre y cuando se le de un manejo adecuado y tenga como propósito especifico almacenar los backup. Pero la realización de estas actividades debe estar acompañada de una definición del plan de backup que involucre la periodicidad, el responsable de ejecutar la tarea o supervisar que se realice, medios de almacenamiento utilizados y rotación de los mismos, en caso de que la empresa lo defina como necesario, se pueden establecer procedimientos de transporte y retención de backup por un tercero; teniendo claro que si esto último se realiza se debe contratar con un tercero de confianza, que sea reconocido en el mercado y con el cual se establezcan acuerdos de confidencialidad y acuerdos de nivel de servicio. Adicional a lo anterior es importante establecer la periodicidad de las pruebas de las copias de seguridad, es decir, los restore de la bases. Lo más apropiado es que se tenga una base de datos de pruebas donde se haga restore del backup seleccionado y se establezca un set de pruebas donde se pueda verificar que el backup es funcional y que la información ha conservado integridad.
Para el motor de base de datos no sobra que se implementen controles extras como software analizadores de líneas base o controles de buenas prácticas indicadas por el fabricante.

5. Controles Físicos
Cuando la empresas adquiere SAP Business One, es necesario que adquiera o disponga de un servidor para instalar el sistema. Algunas empresas se deciden por implementar una solución de servidor en alquiler, sin embargo una gran mayoría decide adquirir el servidor físico y disponer un espacio en sus instalaciones para este. Para lo cual es importante tener presente que este servidor no se debe dejar en un área de fácil acceso, de ser posible se debe dejar en un espacio donde se tenga algún control de acceso y donde solo personas autorizadas puedan ingresar.

Además del lugar que se designe también es necesario que se ubique el servidor en un rack, de manera que este protegido frente a cualquier incidente que pueda ocurrir en las instalaciones. Los respaldos de corriente eléctrica son fundamentales y no los podemos omitir ya que la probabilidad de cambios o interrupciones de corriente eléctrica en la mayoría de las empresas es muy alta y este tipo de fallas puede generar un impacto bastante alto en cuanto a la información almacenada, es muy común que este tipo de fallas originen daños en los discos duros o que la base de datos sufra alteraciones o afectaciones al perder conexión durante procesos de consulta o ingreso de información. Se recomienda que como respaldo de corriente eléctrica se utilicen UPS inteligentes, que generen alertas a los funcionarios encargados de apagar el servidor cuando se presenten caídas de corriente en horarios no laborales o incluso que tengan la opción de apagar de manera controlada el servidor en los casos mencionados.

6. Otros Controles
Los sistemas ERP como SAP Business One son operados por personas y aunque trabajen sobre plataformas tecnológicas y las empresas se enfoquen en asegurar cada componente

tecnológico de la estructura, al final las personas son las que ingresan, modifican y consultan la información del sistema. Por esto es importante que las empresas no olviden que dentro de las medidas de seguridad se debe contemplar al factor humano, al cual se debe capacitar debidamente para hacer uso del sistema; no solo en la fase de implementación, a través del tiempo es importante que se realicen retro alimentaciones del sistema y se establezca un marco de mejora continua. Otro de los aspectos importantes en cuanto al factor humano es su estado, se tiene que tener un equipo de trabajo motivado para que realice su trabajo sin ser afectado por factores externos.

7. Conclusiones

Al realizar una considerable inversión en un sistema como SAP Business One es importante que las empresas se concienticen en la obligación que tienen para establecer medidas y controles que brinden seguridad a su información. Esta serie de sugerencias se pueden llevar a cabo, en su gran mayoría, sin tener un área de tecnología organizada. La implementación de una serie de controles que en algunos casos pueden pensarse que son lógicos, pero que en muchos casos no se aplican, pueden ayudar a las empresas a mitigar los nuevos riesgos que aparecen cuando toda la información de la empresa empieza a fluir a través de un ERP.

Muchos de los controles o medidas sugeridas se pueden implementar sin grandes conocimientos en tecnología, incluso sin ser expertos en el SAP Business One. Sin embargo, la implementación de cada control demanda tiempo y mucha responsabilidad ya que estos temas no se pueden tomar a la ligera y deben realizarse a conciencia, con la premisa de que la inversión de tiempo que se realice en el desarrollo de estas actividades, se justificara en la medida en que se eviten incidentes que pueden causar un gran impacto al interior de la organización.

Muchos incidentes de seguridad ocurren en las empresas por funcionarios descontentos, inconformes, con sobre carga laboral o simplemente por errores humanos. Dichos incidentes que pueden ser con o sin intención pueden generar problemas que impacten a la empresa directamente. Uno de los objetivos es que este tipo de incidentes se identifiquen y logren minimizar su impacto.

Seguramente la implementación de controles de seguridad desde el interior le brindara a la empresa una estructura mucho más organizada y podrán hacer uso del sistema con una mayor confianza en que la información que se registra tiene un respaldo y esta siendo accedida por las personas autorizadas. De esta manera si la empresa tiene una estructura interna podrá implementar controles para evitar o mitigar ataques externos con más facilidad.

Es indispensable que las empresas no realicen la implementación de los controles una única vez, pues de este modo no seguramente los riesgos se materializaran en algún momento, por lo que la gestión debe ser un proceso responsable y que pueda llevarse a un nivel de madurez cada vez más alto. Es importante que se realice un seguimiento a los incidentes de seguridad que ocurran relacionados con el sistema, llevar una bitácora y realizar un estudio periódico sobre la información reunida para evaluar que clase de incidentes ocurren, que característica de la información afecta, con que frecuencia se presentan, si se han utilizado controles y si estos controles han sido efectivos. Aquí se menciona una idea muy corta de lo que seria una gestión de riesgos dentro de una empresa.

8. Referencias

[1] Verizon 2014 Data Breach Investigation Report, 2014.

[2] ESET Security Report 2014, 2014.

[3] NIST special publication 800-30 – Risk Management Guide for Information Technology Systems, 2002.

[4] NIST special publication 800-30 Revision 1 – Guide for Conducting Risk Assessments, 2012.

[5] Sistema SAP Business One Versión 9.0 PL 10, 2014.