

Seguridad en SAP: sepa cómo mantenerla controlada

POR ANIBAL MASTROBERTI, CONSULTOR CYBSEC S.A.

Uno de los principales objetivos e intereses de una empresa es mantener a salvo la información de negocio a personas o sistemas indeseados. Gran cantidad de las principales empresas, en su mayoría, grandes y medianas han implementado diversos sistemas informáticos que permiten facilitar su gestión y optimizar el uso y el proceso de transformación de su información de negocio entre distintas las diversas áreas que la componen mediante la utilización de un sistema ERP (Planificación de Recursos Empresariales).

En particular en este artículo se va a considerar uno de esos sistemas ERP creado en el año 1992 por la empresa Alemana SAP AG denominado SAP R/3 (existen diversidad de versiones previas y posteriores). SAP R/3 es una aplicación cliente – servidor. Esto quiere decir, que para poder utilizar el sistema, se tiene que instalar un programa (cliente) y ese programa es el que realiza el acceso al sistema ERP de SAP, que se encuentra instalado en un servidor. Se va a explicar como está compuesta una de estas partes del sistema (servidor), haciendo una separación en distintas capas en las que se puede subdividir.

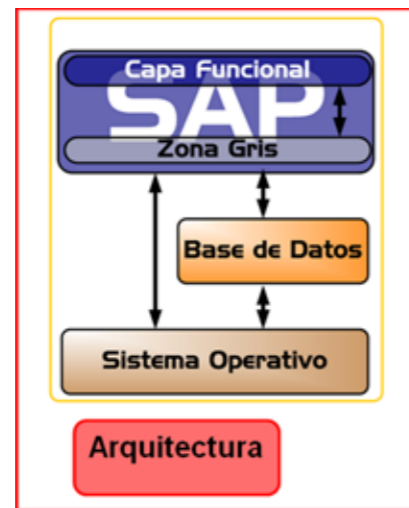
Capa Funcional

Esta capa contiene la lógica de negocio, que puede separarse en diversos módulos, que se diferencian por el proceso de negocio o área funcional que abarca cada uno. Por ejemplo existe un módulo de finanzas, conocido y denominado por la sigla FI; un módulo de ventas y distribución denominado SD, entre tantos otros. Se pueden agrupar estos módulos en grandes áreas (financiera, logística y recursos humanos) y funcionan de un modo integrado, por necesidad de interacción en los distintos procesos de negocio.

Cada empresa, decide ‘implementar’ o instalar y configurar o parametrizar los módulos que se adapten a su operatoria y en algunos casos adaptar la operatoria de la empresa los procesos estandarizados de cada módulo. El concepto de parametriza-

ción hace que un determinado módulo, se adapte a las necesidades de los procesos de una empresa y forma parte de lo que se puede llamar como una capa de Zona Gris, que se explicará luego. Toda la información utilizada por la Capa Funcional, se encuentra guardada dentro del sistema en distintas tablas y

Capas del sistema SAP



objetos en una gran Base de Datos.

La **Zona Gris** consiste en la parametrización/configuración específica que se realiza tanto en la Capa Funcional, como en el mismo sistema SAP R/3 a nivel de Sistema Operativo, para su adecuado funcionamiento. La **Base de Datos** es el lugar donde se guarda la información utilizada por la Capa funcional y parte de la información denominada Zona Gris (Configuración). Para la instalación tanto de la Base de Datos, como el aplicativo SAP R/3, se requiere tener instalado primero un **Sistema Operativo** en el servidor que se utilice.

Idealmente, se instalan tres ambientes de trabajo distintos de un mismo sistema SAP (Desarrollo, Testing / QA y Producción). En el gráfico, se muestra un diagrama donde se modela la arquitectura que se aconseja para infraestructuras de SAP.

Seguridad en el Sistema SAP

La información de negocio de las empresas que utilizan SAP, se encuentra guardada dentro del mismo sistema. Es por eso, que es primordial asegurar y restringir el acceso, solamente a la/s persona/s que deben tener conocimiento de parte de la información que les sirva para realizar su trabajo utilizando el sistema. Dentro de las consideraciones que se deben tener en cuenta para hacer esta restricción en las distintas capas mencionadas, es que existen muchas configuraciones por defecto y la gran mayoría, son inseguras dentro del sistema. A continuación, hace un análisis por capa de la seguridad necesaria en cada una.

Seguridad en la Arquitectura

Los servidores que formen parte de la infraestructura SAP deben estar en una red aislada, en particular lo que es conocido como SAProuter y la infraestructura de SAP dentro de una DMZ. Una DMZ es una zona de la red que se mantiene separada de la red empresarial y de las redes externas. De esta forma, se realiza el acceso desde el exterior en forma segura a la infraestructura SAP. Este acceso es necesario para el Soporte Directo realizado por parte de SAP.

Esta separación permite limitar las conexiones que se hagan al sistema, permitiendo únicamente el uso de aquellas autorizadas. Se pueden implementar estas restricciones de acceso utilizando un Firewall (rechaza conexiones indebidas) y el uso de la aplicación mencionada SAProuter, que permite además restringir el acceso a la infraestructura SAP (ver diagrama de arquitectura).

Seguridad en Sistemas Operativos

- Seguridad en las cuentas de acceso:

Como el sistema SAP, se instala en un Sistema Operativo, se debe limitar el acceso y uso, solamente para hacer tareas de instalación y actualización del sistema a personas especializadas (Basis). Se deben utilizar políticas que defina la empresa, para el ingreso al



La solución integral para tus proyectos



En DACAS encontrarás

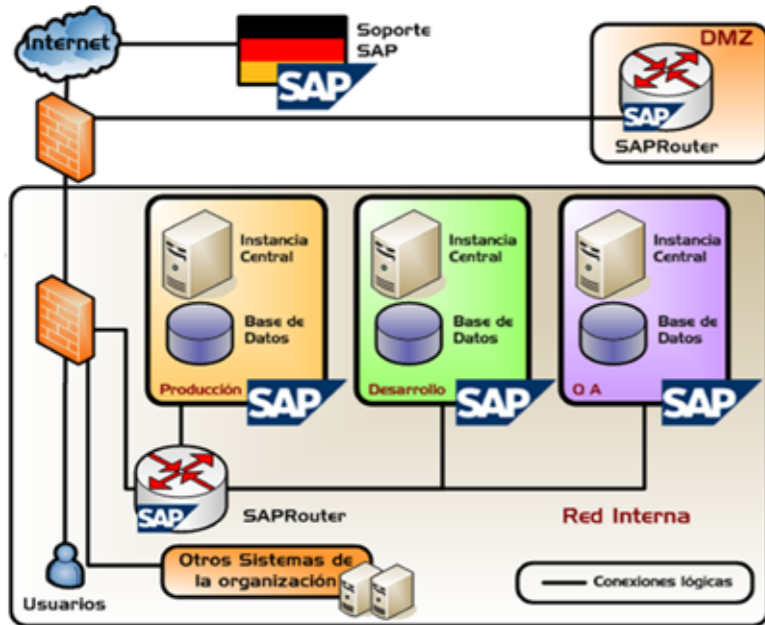
- Atención Personalizada
- Staff Altamente Capacitado
- Servicio Pre-Post Venta
- Disponibilidad de Stock local
- Amplia gama de Soluciones
- Capacitación Permanente al Canal
- Logística
- Servicio de RMA
- Soluciones end to end

Dacas Argentina: Nuñez 3481 - Ciudad Autónoma de Buenos Aires - (54-11) 4545-3900 - e-mail: ventas@dacas.com
 Dacas Uruguay: Durazno 875 - Montevideo - (598-2) 900-7784 - 901-5696 - e-mail: montevideo@dacas.com

www.dacas.com

Seguridad en SAP: sepa cómo mantenerla controlada

Arquitectura SAP



sistema operativo, la definición de contraseñas a usuarios administradores del sistema Operativo y usuarios especiales creados al instalarse SAP. Se debe buscar siempre, limitar al máximo el ingreso indebido.

- Seguridad en el sistema de archivos

Así como se limita el ingreso al sistema operativo, se debe restringir el acceso a carpetas y archivos mediante la asignación de permisos a los usuarios del sistema operativo.

- Seguridad en servicios

Se deben desactivar los servicios del Sistema Operativo, que no se utilicen y sean necesarios para el funcionamiento del sistema SAP, por ejemplo: smtp, ntp, telnet, snmp, ftp*, rsh*, rexec* y rlogin*.

- Estandarizar el nivel de seguridad

La empresa debe definir un standard de seguridad para el Sistema Operativo y utilizarlo para todos los ambientes (Desarrollo, Testing y Producción).

Seguridad en Base de Datos

- Seguridad de usuarios

Los usuarios que tiene y utiliza la Base de Datos, se deben proteger, cambiando las contraseñas en los usuarios creados por defecto y creados por el sistema SAP para el uso de la Base de Datos.

- Restringir accesos indebidos

Limitar el acceso directo a la Base de Datos, permitiendo únicamente el acceso al sistema Aplicativo SAP y restringir el uso de cuentas administrativas.

- Limitar acceso a archivos de la Base

Se deben aplicar los permisos adecuados a los directorios donde se guarda la información de la base de datos.

Seguridad en la Zona Gris

Es una zona compuesta por diversas configuraciones y parametrizaciones que se realizan dentro del sistema. En algunos casos son configuraciones por defecto y en general inseguras. Se detallan las agrupaciones de los distintos conceptos que forman esta Zona Gris:

- Mecanismos de Autenticación

Es la forma en que se acredita un usuario al tratar de ingresar al sistema SAP y existen diversos mecanismos. El más común es ingresar utilizando un usuario y contraseña, como se explicó previamente. Es recomendable utilizar un mecanismo de comunicación seguro utilizando SNC (Secure Network Communications), que es provisto por SAP.

- Seguridad de los Usuarios

Se deben cambiar las contraseñas de los usuarios creados por defecto por el sistema SAP (SAP*, DDIC, EARLYWATCH) y tomar

medidas preventivas en el uso de estos usuarios críticos.

- Política de Contraseñas

La empresa debe definir una política de contraseñas para evitar el uso de contraseñas triviales, al momento de realizar asignaciones de contraseñas para el acceso al sistema.

- Mecanismos de Autorización

Son las autorizaciones que se dan al usuario para poder utilizar objetos del sistema. Es aconsejable restringir el uso necesario a los objetos que requiera cada usuario para su trabajo. Limitar el uso del perfil SAP_ALL, que tiene privilegios total sobre el sistema y controlar la asignación de autorizaciones administrativas S_*

- Seguridad de las Interfaces

Controlar y restringir las comunicaciones innecesarias con otros sistemas, el acceso a los usuarios a hacer esta configuración y utilizar SNC en lo posible para hacer las comunicaciones seguras en caso de transmitir información sensible.

Seguridad en la Capa Funcional

Se debe restringir el uso de la funcionalidad que debe acceder cada usuario en el sistema. Para esto existe el uso de asignación de roles, perfiles y autorizaciones de objetos que puede utilizar un determinado usuario. Es importante limitar e identificar los usuarios que cuenten con estos permisos administrativos, de asignación de permisos y que la asignación a los distintos usuarios creados se haga de forma correcta. También limitar la asignación de autorizaciones para realizar parametrizaciones dentro del sistema a los usuarios creados dentro de SAP que correspondan.

Manteniendo la seguridad bajo control

Con intención de mejorar la seguridad dentro de SAP de lo que se dio a conocer como Zona Gris, existe una herramienta que realiza un exhaustivo análisis de los parámetros de instalación. Es una aplicación que automatiza más de 80 controles críticos dentro del sistema SAP y NetWavere y los compara con las best practices internacionales indicando el valor objetivo a alcanzar. Para obtener más información sobre esta herramienta puede visitar el sitio www.cybsec.com/safe



Distribuidor Oficial

En Video IP no todo es lo mismo.

Da en el blanco comprando a los que saben.



Atención Personalizada / Asesoramiento Técnico / Experiencia en Seguridad Electrónica.



Salto Cualitativo

Hacia una velocidad de transferencia 10 veces mayor de los cableados estructurados

POR CÉSAR MANGIATERRA, LEONARDO FUHR, DUSAN VANEK, MICHAL SOBOLIC, PAVEL NEVESELÝ, P. VACEK, L. DÖBRÖSSY

SEGUNDA PARTE

En el número anterior hicimos un repaso de la evolución de los cableados estructurados. Analizamos tres 'hitos' de tal proceso. El pasado 15 de abril, la norma internacional ISO/IEC 11801 publicó su segunda enmienda. A partir de ahora, no sólo se especifican los requerimientos para sistemas Cat.6A, sino también los parámetros de transferencia (y la forma de testarlos y certificarlos) de cada uno de los componentes Cat.6A. La característica más importante de estos componentes: la interoperabilidad.

Dos vías para la realización de un cableado estructurado Cat.6A. Estamos frente a una nueva etapa, en la que los cableados Cat.6A se podrán construir de dos modos: mediante la instalación de todo un sistema Cat.6A, o instalando componentes Cat.6A con interoperabilidad. Ambas posibilidades tienen el mismo valor y están respaldadas por las normas internacionales.

El rol de los certificados para los sistemas y los componentes Cat.6A. La categoría de performance 6A está garantizada tanto a nivel sistema como a nivel componente Cat.6A sólo en el caso de responder a las

normas a las cuales nos hemos referido. Esto es imposible de demostrar de otra manera que con pruebas y mediciones que sólo se pueden realizar en laboratorios de prueba especializados.

El cliente es capaz de diferenciar los verdaderos sistemas y componentes Cat.6A de los falsos de gracias a los certificados emitidos por laboratorios de pruebas independientes. Por eso, debe ser una regla solicitárselos al proveedor sin excepciones. En el caso de un sistema Cat.6A se trata de un certificado para todo el canal de transmisión y en el caso de los componentes Cat.6A, cada uno de éstos está certificado por separado (o, eventualmente, en grupos de una misma línea de productos). Para saber si se trata de un sistema Cat.6A, un elemento constitutivo de sistema un Cat.6A o un verdadero componente Cat.6A es importante prestar atención a los textos y datos que constan en los certificados.

El rol de las certificaciones para los sistemas y los componentes Cat.6A. Las mediciones de certificación del cableado instalado mediante instrumental portátil (testers) tienen como fin verificar la calidad del trabajo de instalación y la detección

de eventuales fallas. Pero de ningún modo reemplazan a un certificado de sistemas o de componentes Cat.6A emitido por un laboratorio de pruebas independiente (ver el punto anterior).

Para la certificación del cableado instalado Cat.6A es indispensable utilizar instrumental con categoría de precisión IIIe o IV con generador de frecuencia de por lo menos 500 MHz. Si se trata de un sistema completo Cat.6A, siempre hay que testarlo como canal (Channel) usando patchcords correspondientes al sistema dado. De tratarse de un cableado realizado con componentes con interoperabilidad Cat.6A tenemos dos opciones: realizar la medición como canal (de la misma forma que para un sistema Cat.6A) o como enlace permanente (*Permanent Link*). La segunda opción presenta la ventaja de que al momento de realizar la distribución, no es indispensable definir un tipo concreto de patchcord, ni su fabricante (lo que en la mayoría de los casos no se puede asegurar). La categoría de performance está garantizada para todos los patchcords Cat.6A sin necesidad de medición o verificación complementaria.

Todos los instrumentos de medición presentan, además de la norma internacional, la norma nacional TIA/EIA válida en los EE. UU. En principio, ésta emana de soluciones no apantalladas y por eso las exigencias para las características de transmisión de los componentes y de los sistemas son menores. Es por eso que es necesario seleccionar siempre en los testers la norma ISO/IEC 11801. Las excepciones son: instalaciones realizadas en los EE. UU., instalaciones realizadas en países cuya norma nacional emane de la TIA/EIA-568, instalaciones realizadas en sedes, sucursales o filiales de firmas estadounidenses localizadas en otros países.

Análisis y calificación crítica de los mercados

Motivos de la 'táctica del avestruz'. A pesar de que hace casi tres años que está

DOS VÍAS PARA LA REALIZACIÓN DE UN CABLEADO ESTRUCTURADO CAT.6A



45U

RACK PREMIUM SERVER 19"



SOLUCIONES EN FIBRA OPTICA





Salto Cualitativo - Segunda parte

LA TÁCTICA DEL AVESTRUZ



claro que instalar Cat.6 no tiene sentido, en muchos mercados éste cableado sigue siendo un bestseller. Los argumentos de utilizar la Cat.6 en lugar de la Cat.5E son engañosos, toda vez que la velocidad de transmisión 1 Gbit/s está garantizada para la Cat.5E por la norma y el ancho de banda de 100 MHz fue adoptado ya teniendo en cuenta un 20% de margen.

A un cliente menos exigente tiene sentido ofrecerle una solución Cat.5E, y a un usuario que necesite un cableado con alta performance y que soporte futuras aplicaciones de alta velocidad, una Cat.6A. Analizando la situación en varios mercados hemos observado que el retraso en la incorporación al mercado de la categoría 6A guarda directo correlato con la porción de éste correspondiente a los sistemas no apantallados. Podemos interpretar esto como un freno intencional al desarrollo de parte de algunos abanderados de los cableados no apantallados.

Entre otros factores que frenan la incorporación de cableados Cat.6A podemos citar: mayor peso y agresividad mercadotécnica de los fabricantes que hasta el mo-

mento no disponen de soluciones Cat.6A (los llamados 'followers' sin base de desarrollo propia, que tratan de imitar y copiar productos originales); interés comercial de los principales fabricantes de obtener por el mayor tiempo posible ganancias con la comercialización de portafolios Cat.6 y así darle más valor a las instalaciones e inversiones llevadas a cabo en el pasado; ausencia de información calificada sobre los productos al momento de la venta a través de canales de distribución modernos (ventas por internet, mayoristas, cadenas comerciales); grandes licitaciones y compras centralizadas para el sector estatal y corporaciones internacionales redactadas de acuerdo a la inercia basada en reglamentaciones internas anticuadas para la construcción de infraestructuras de datos de la organización; desinterés o incompreensión de la necesidad de la frecuente actualización de conocimientos de

los proyectistas de los sistemas de cableado estructurado; y posición interesada y necia de algunas firmas instaladoras con respecto a sus clientes ('Si hoy instalo Cat.6, en algunos años va a necesitar que le instale Cat.6A').

El mayor desplazamiento hacia la Cat.6A se produce sobre todo gracias al trabajo conjunto de las firmas consultoras inmobiliarias, que recomiendan invertir en edificios teniendo muy en cuenta la calidad y escalabilidad de la infraestructura IT de los espacios a ocupar. También se aliaron muchas firmas instaladoras e integradoras de IT. Éstas concluyeron en que perseverando en la plataforma Cat.5E y Cat.6 serían progresivamente desplazadas del negocio por empresas instaladoras de energía eléctrica, las cuales pueden realizar las instalaciones de tales categorías en forma simple y sin su ayuda.

Los componentes de un sistema Cat.6A no son componentes Cat.6A

LOS CAMBIOS EN EL CONOCIMIENTO Y LA NORMALIZACIÓN INTERNACIONAL DURANTE LOS ÚLTIMOS AÑOS SE PUEDEN RESUMIR EN LOS SIGUIENTES PUNTOS:

1. Desde el punto de vista normativo, para establecer los requerimientos de una vía de transmisión (cableado) es decisivo tener en cuenta el protocolo de transferencia
2. Ethernet domina y marca el rumbo del desarrollo de las comunicaciones LAN.
3. El ancho de banda dejó de ser el criterio para la categorización de la performance del cableado y fue reemplazado por la velocidad máxima de transferencia que es capaz de soportar.
4. En la realidad, son relevantes la Cat.5E (para la transmisión de 1 Gbit/s) y la cat.6A (para velocidades de hasta 10 Gbit/s).
5. Las categorías 6 y 7 son 'zombis' y, desde el punto de vista de la performance están al mismo nivel que la Cat.5E (transferencia garantizada sólo hasta 1 Gbit/s).
6. Desde el 2006 es posible realizar cableados con performance Cat.6A con soluciones sistémicas Cat.6A.
7. Algunos componentes Cat.6 y Cat.7 de calidad pueden ser utilizados como componentes constitutivos de sistemas Cat.6A.
8. Desde 2009 existen los componentes Cat.6A y su característica básica es la interoperabilidad.
9. Tanto las soluciones sistémicas cat.6A y las soluciones constituidas con componentes Cat.6A son equivalentes y están respaldadas por las normas internacionales.

¿Quiere leer **Prensario TI Latin America** el día de su salida?

- Todos los meses
- Desde cualquier punto de América Latina

Ingrese a www.prensariotila.com y descargue la revista completa en formato PDF



CONECTANDO SUS NECESIDADES CON LAS SOLUCIONES MÁS INTELIGENTES

Anixter es distribuidor de productos de múltiples fabricantes para soluciones de infraestructura en redes de voz, datos, video y seguridad, todas soportadas por los servicios integrales de la cadena de suministro.



Anixter Argentina S.A.
 Castro 1844/46 (C1237AAP), Ciudad de Buenos Aires
 Tel.: (54-11) 4909-5200 / Fax (54-11) 4909-5265 / 0810-22 ANIXTER
www.anixter.com | info@anixter.com.ar

