**ACTIVIDAD 3**

**CONTROLES DE TI**

**Estudiante: Daniel Vargas Rios**

**Asuma que usted realiza una revisión de seguridad de TI de infraestructura crítica en una entidad financiera (Banco) con un nivel de madurez entre 4 y 5.**

1. **Qué infraestructura crítica mínima considerará en la revisión?. Para ello esquematice similar a lo visto en clases, SO, BD y Aplicación(es) e indique qué versiones de SO y BD.**

Se debería de considerar las versiones y que tipo de software se usan, ya que si se llega a usar una versión antigua es muy propensa a tener vulnerabilidades o huecos que no fueron corregidos con el tiempo. Este punto a revisar es valido tanto para el SO como para el tipo de BD que se usa, doy el ejemplo de una entidad cuya BD esta basada en FoxPro, este mismo es muy viejo y poco recomendado ya que no tiene un buen soporte como otras aplicaciones.

Siempre es recomendable que se use un SO enfocado a servidores como lo es Windows Server y no versiones domesticas como Windows Home/estudiantil o similares. El servidor de base de datos debe ser restringido y dedicado, al decir dedicado me refiero a que ese mismo equipo no se valla a usar para otro fin que no sea alojar la base de datos, y evitar que lo usen para usar el navegador, hacer consultas web, etc.

Para el sistema ERP es muy diverso y debe tener obligatoriamente controles de acceso y parámetros establecidos para cada usuario, sabe destacar que el servidor donde se aloja el mismo sistema ERP también debe ser dedicado y el mismo equipo no debe ser usado para otro fin que no sea alojar el sistema ERP. El mismo sistema debe contemplar medidas de seguridad y evitar tener códigos o contraseñas establecidas dentro de la programación.

Otro aspecto que también es importante es que los mismos servidores de aplicaciones y base de datos, deben estar separados y resguardados en una sala donde solo se pueda acceder con una previa autorización, en el caso que estuviera en una sala o dentro de la oficina de un jefe o directivo, ya seria algo grave para una infraestructura de nivel 4.

Los accesos al sistema y a la base de datos es un tema importante, estos mismos deben estar parametrizados y limitados según las funciones del personal, y en el caso de ser para una reestructuración o editar/modificar algún parámetro del mismo, debe ser bajo doble supervisión y que requiera la contraseña de dos personas para ingresar.

2. **Describa cómo usted encararía la revisión del punto anterior (es decir cuál sería el paso a paso que consideraría). Si gusta puede asumir que es un consultor externo contratado para dicha revisión o que es un Oficial de Seguridad de la Información.**

Lo primero que realizaría es:

- Obtener un listado organizado de los activos de información de la entidad
- Comprobar si de alguna manera los equipos del área de soporte o desarrollo pueden acceder, y si al acceder que privilegios tienen. (Importante, los equipos deben estar segmentados en la red)
- Revisar si los equipos están actualizados a la fecha.
- Comprobar los niveles de seguridad en la contraseña e inicio de sesión de los diferentes usuarios que tiene la entidad.
- Aplicar técnicas CAAT entre los servidores de aplicación y DB para confirmar existe una correlación entre lo que se escribe y lo que se envía.
- Auditar el sistema ERP y comprobar que exista las medidas necesarias de seguridad para la información (Es parametrizable, si cuenta con módulos de seguridad, si tiene tablas que realizan la confirmación de errores por métodos matemáticos)
- Obtener un listado de las modificaciones que se hayan realizado en el sistema o DB.
- Comprobar que lo que este documentado y lo que se obtiene al auditar el SO o DB, exista una relación.
- Revisar que los servidores estén separados de las otras áreas y comprobar quienes son los que tienen acceso a la sala (ya sea por una tarjeta de identificación, contraseña o llave).
- Comprobar cuales son los controles que se implementan para poder acceder a los servidores.

3. **En la revisión de parámetros de seguridad (por ejemplo de contraseñas) de los sistemas (SO, BD, Aplicación) qué aspectos consideraría en la revisión?**

Lo mas esencial es revisar si existe algún método o medida para parametrizar la misma, ya sea por limite de caracteres, cantidad de intentos fallidos, evitar que la contraseña sea la misma que las anteriores.

Otro factor importantes es confirmar que no exista una contraseña por defecto o uso para desarrollo que solo la sepa una persona, o sea, en el caso que la persona que da soporte a la base de datos de

la entidad sea una empresa, esa empresa no debe tener la contraseña para poder modificar la DB, porque podría hacerlo para otros fines no éticos, por lo que lo recomendable es que sea una contraseña compartida, los primeros caracteres lo sepa la empresa que da el soporte y los últimos lo sepa la entidad financiera.