POLÍTICA DE DESARROLLO

La presente política será de obligado cumplimiento para todos aquellos proveedores de servicio IT que, desarrollen e implementen aplicaciones, software, herramientas, etc. y/o los cambios de las versiones correspondientes, que puedan comprometer la seguridad e integridad de la información en **CLÍNICA BEIMAN**.

El desarrollo de la aplicación y de los controles de seguridad necesarios deben llevarse a cabo teniendo en cuenta una serie de principios de seguridad que traten de reducir la probabilidad de la realización de amenazas y el impacto de éstas en el caso de que se hayan producido ya.

Los requisitos considerados son los siguientes:

- Seguridad por defecto. Cuando una aplicación se despliega en su entorno de producción, utiliza una serie de opciones de configuración que se establecen por defecto. Estas opciones por defecto deben ser tales que la aplicación sea segura, por defecto una aplicación debería tener habilitada la expiración de contraseñas y una política de complejidad de claves adecuada.
- Ejecución con los mínimos privilegios. El principio de mínimos privilegios establece que las cuentas deben tener el menor nivel de privilegios posible para realizar las tareas de negocio. Este nivel de privilegios abarca tanto permisos de usuarios como permisos sobre recursos como CPU, memoria, red, sistema de ficheros, etc.
- Defensa en profundidad. Una aplicación deberá implementar a distintas medidas en varias capas para prevenir inyecciones SQL.
- Detección de intrusos. La detección de intrusiones requiere la existencia de tres elementos:

    - Capacidad para incluir en el log eventos relevantes de seguridad.
    - Procedimientos que aseguren que los logs son monitorizados con regularidad.
    - Procedimientos para responder adecuadamente a una intrusión una vez ha sido detectada.

- Toda la información de seguridad relevante debe ser registrada en un log.
- Evitar la seguridad por ocultación. La seguridad por ocultación es un mecanismo de seguridad débil y generalmente falla cuando es el único control existente. La seguridad de un sistema nunca debe recaer en la ocultación de secretos (no puede depender de mantener en secreto el código fuente).
- Solucionar correctamente los problemas de seguridad. Una vez que se ha detectado un problema de seguridad, es fundamental desarrollar pruebas para reproducirlo y detectar la causa raíz. Una vez que se desarrolla una solución válida es clave garantizar que no se introducen problemas de regresión.

BENJAMÍN RUIZ CARMONA
Dirección