Capítulo 4.

Lineamientos de Seguridad para lograr la Confiabilidad y Calidad del Software basado en Internet.

En este capítulo plantearemos una serie de lineamientos, estos ayudarán a los investigadores del CENTIA para que sus Aplicaciones Web sean cada vez más seguras y confiables y que al mismo tiempo ofrezcan calidad al usuario. Estos lineamientos pueden ser planteados en la práctica, ya sea al inicio, en el desarrollo o al final de la construcción de una Aplicación Web.

3.1. Planificar la Seguridad.

La planificación de la seguridad es la etapa en donde se realiza la identificación actual de los recursos informáticos, los alcances de los servicios que estos brindan a los usuarios a nivel de aplicaciones, con lo cual se hace una proyección en base al crecimiento de los servicios que se ofrecen, identificando los requerimientos necesarios para implementar y controlar el funcionamiento del mismo. Para lo cual se deben tener en cuenta las siguientes consideraciones **[Romero, 1999]**:

Acciones.

- Demostrar que los costos de los recursos de seguridad están entendidos e incorporados en la planeación del ciclo de vida del sistema.
- Incorporar un plan de seguridad que comprenda:

    1. Las reglas de utilización del sistema y las consecuencias al violar dichas reglas.
    2. Los métodos para identificar, limitar apropiadamente, y administrar los límites de las interconexiones con otros sistemas y los procedimientos específicos para vigilarlos.
    3. Procedimiento para el monitoreo de la eficacia de los controles de la seguridad.
    4. Plan de contingencia en la presencia de un ataque o accidente.

3.2. Alinearse a la Arquitectura de información de la Institución.

Define la necesidad de considerar dentro de la infraestructura física y funcional de los sistemas de información, el desarrollo de un plan de seguridad en función al crecimiento de esta arquitectura **[Romero, 1999]**.

Acciones.

- Los controles de la seguridad para los componentes, las aplicaciones, y los sistemas deben ser parte integral de la arquitectura tecnológica de los sistemas de información de la institución.

3.3. Tomar control de los riesgos.

Los riesgos son constantes y se necesita tener los mecanismos necesarios para analizarlos y posteriormente aplicar las estrategias precisas frente a estos riesgos, y no esperar a que ocurran para construir una solución.

Acciones.

- Establecer un método específico y entendible para evaluar continuamente los riesgos potenciales, con la finalidad de mantener la seguridad a un nivel aceptable, así como los procedimientos para asegurar un control eficaz con los tiempos de respuesta necesarios.
- Identificar de ser necesario controles adicionales de seguridad para reducir al mínimo el riesgo potencial de pérdida de los sistemas a promover o permitir acceso público.

3.4. Proteger la privacidad.

Es necesario el establecimiento de mecanismo que ayuden a proteger la privacidad, que realizan comunicación para acceder al uso de recursos de información de las entidades públicas **[Castillo, 2004]**.

Acciones.

- Mantener herramientas eficaces para el control de la seguridad.
- Asegurar que la información personal este respaldada por políticas del gobierno.
- Controlar las aplicaciones y la información a que tienen acceso los usuarios y cómo pueden llegar hasta ellas. Controlar quien puede abrir cuentas o crear identificaciones de usuarios en un sistema, auditar las cuentas con frecuencia en busca de identificaciones o cuentas que no corresponden a la realidad de tener a manos personas capaces de llevar a cabo una auditoría.

3.5. Mantener estándares de seguridad.

Los estándares en informática son las recomendaciones técnicas que facilitan una mejor administración y crecimiento de los recursos informáticos de información a nivel nacional.

Acciones.

- Para la seguridad de las aplicaciones, asegurar el uso de estándares, al implementar productos y herramientas.
- Usar productos de seguridad disponibles y probados en el mercado. Los productos basados en estándares abiertos han sido probados y aprobados. Lo más importante de todo es que los productos estandarizados de la industria están de modo típico, bien documentados para que se empleen bien.

3.6. Mantener simple para los usuarios la implementación de los planes de seguridad.

Si el sistema es muy complicado, los usuarios lo evitarán o tratarán de darle un rodeo con lo que se anularán las medidas se seguridad y se reducirá su utilidad, las medidas de seguridad modernas pueden ser efectivas sin interferir.

3.7. Desarrollar y cumplir de forma proactiva políticas, procedimientos y sanciones.

Se deben establecer métodos para tener la certeza de que las políticas de seguridad establecidas, se están cumpliendo correctamente.

Acciones.

- Diseñar un sistema de seguridad que se base en las necesidades del usuario, la naturaleza de las aplicaciones y la información que se asegura.
- Aplicar medidas de seguridad constantemente, pues tener políticas de seguridad que no se aplican es peor que no tener ninguna.

3.8. Probar, auditar, inspeccionar sitios e investigar continuamente.

La seguridad de la información es una actividad constante y necesita del establecimiento de acciones continuas, por ellos es necesario tomar en cuenta consideración las siguientes acciones **[Castillo, 2004]**:

Acciones.

- Realizar de forma periódica análisis de vulnerabilidades de los sistemas de información para protegerse de las amenazas internas y externas.
- Usar una metodología para examinar y probar códigos para bloquear las puertas traseras de los sistemas informáticos.

- Usar un sistema de auditoría automática y programas de vigilancia.
- Dar a conocer las amenazas y las respuestas que se les da.

En este capítulo se plateó una serie de lineamientos para apoyar a los investigadores del CENTIA a tener un desarrollo de Aplicaciones Web más seguras. Poniendo en práctica estos lineamientos se puede llegar a tener una seguridad de las Aplicaciones Web aceptable.