ANEXO No. 20 NORMAS PARA DESARROLLO DE SISTEMAS

1. Requerimiento de Seguridad

Antes de iniciar el proceso de desarrollo y/o implementación de los sistemas de información se debe identificar y acordar los requerimientos de seguridad. Todos los requerimientos de seguridad se deben identificar en la fase de requerimientos del proyecto y deben ser justificados y documentado como parte del caso comercial general.

2. Análisis y especificación de los requerimientos de seguridad

Los requerimientos y controles de seguridad deberían reflejar el valor comercial de los activos de información involucrados y el daño comercial potencial que podría resultar de una falla o ausencia de seguridad.

Si se desarrolla un sistema o producto de software y se comprueba que causa algún riesgo de seguridad se debe revisar la estructura de control propuesta para determinar si se puede solucionar o disminuir el riesgo asociado

3. Seguridad de las aplicaciones del sistema

Se requerirán controles adicionales para sistemas que procesen o tengan impacto en información sensible, con mucho valor o críticas. Estos controles deben ser determinados en base a los requisitos de seguridad y la evaluación de riesgos.

4. Validación de los datos de entrada

Se debe aplicar las reglas de validación para la captura de datos, siguiendo los siguientes controles:

4.1 entradas duplicadas, datos incompletos, datos con estructura especifica como campos delimitados o compuestos con el fin de detectar errores como:

a. Valores fuera de rango.
b. Caracteres invalidados.
c. Datos que faltan o están incompletos.
d. Datos que exceden los límites de volumen por exceso o defecto.
e. Datos de control no autorizados o inconsistentes.

4.2 Revisión periódica de campos claves o archivos de datos con el fin de verificar su validez e integridad.

4.3 Inspección de los documentos físicos de entrada para ver si ha cambios no autorizados a los datos de entrada.

4.4 Procedimientos para responder a los errores de validación.

4.5 Procedimiento para comprobar la integridad de los datos de entrada.

4.6 Definición de las responsabilidades de todos los implicados en el proceso de entrada de datos.

4.7 Creación de registros de auditoria de las actividades envueltas en el procesamiento de los datos de entrada.

5. Control del proceso interno

En la fase de diseño de aplicaciones se debe implementar restricciones con el fin de minimizar el riesgo por fallos en las aplicaciones o por actos deliberado que impacte la pérdida de integridad de los datos.

Se considera áreas de riesgo:

a) Funciones de Añadir, Modificar, Borrar para cambiar datos.

b) El uso de procedimientos para evitar programas que corran en orden equivocado o después del fallo de un proceso anterior o en caso de fallos del sistema.

c) Uso de programas apropiados de recuperación después de fallas para asegurar el proceso correcto de los datos.

d) Protección contra ataques utilizando corridas o desbordes de buffer.

6. Validación de Datos de Salida

Se debe validar los datos de salida de los sistemas de aplicación para garantizar que los datos suministrados sean los correctos y apropiados. Para que el proceso sea confiable se debe determinar los responsables implicados en el proceso de salida de datos además se debe establecer registros de auditoria con el de validar los datos de salida.