Adquisición de sistemas de información, desarrollo y mantenimiento	
Cantidad de objetivos de control	6
Cantidad de controles	16
Total de preguntas	35

12.1 Objetivo — **Requerimientos de seguridad de los sistemas de información**

Asegurar que la seguridad es parte integral de los sistemas de información

12.1.1 — **Análisis y especificación de los requerimientos de seguridad**

Los requerimientos del negocio para los nuevos sistemas de información o la ampliación de los existentes, especifica los requerimientos de control y seguridad

- ○ SI, Todos o la mayoria de proyectos
- ◉ Solo algunos projectos
- ○ NO

Es la gestión del riesgo usada como marco para analizar los requerimientos de seguridad e identificar controles en los sistemas de información

- ○ SI
- ◉ NO

12.2 Objetivo — **Correcto procesamiento en las aplicaciones**

mantener e implementar unos niveles adecuados y acordados de entrega de servicios con terceras partes

12.2.1 — **Validación de datos de entrada**

Es la entrada de datos a los sistemas de aplicación sujeta a control de validación para garantizar integridad, exactitud y autenticidad

- ◉ SI
- ○ NO

Cual de las siguientes no se incluyen en los chequeos de validación

- ☐ Valores fuera de rango
- ☐ Caracteres inválidos
- ☐ Datos incompletado o omitidos
- ☐ Exceder volumen de datos
- ☐ Datos de control no autorizados

Cual de los siguientes controles no son aplicados para garantizar la validez de los datos

- ☐ Revisiones periódicas de archivos/campos claves
- ☐ Inspección de documentos para validar cambios no autorizados
- ☐ Procedimiento de validación de errores
- ☐ Responsabilidad del personal involucrado en la entrada de datos
- ☐ Viabilidad de los datos de entrada

12.2.2 — **Control de procesamiento interno**

Existen chequeos de validación dentro de las aplicaciones que detecten cualquier tipo de corrupción de información

- ◉ SI
- ○ NO

Cual de los siguientes controles de validación no son aplicados para detectar cualquier corrupción de la información

- ☐ Controles de batch o de sesión
- ☐ Validación de datos de entrada generados
- ☐ Validación de integridad/autenticidad entre computadores
- ☐ Hash de archivos
- ☐ Validación de ejecución de tiempo correcto
- ☐ Validación de ejecución en el orden correcto
- ☐ Logs de las actividades involucradas en el procesamiento

12.2.3 — **Integridad de los mensajes**

Es utilizada la autenticación de los mensajes, en la cual se involucra la transmisión de información sensible, para prevenir o detectar cambios no autorizados o corrupción de los datos

- ○ SI
- ○ NO aplicable
- ◉ NO

12.2.4 — **Validación de datos de salida**

Son las salidas de datos de las aplicaciones validadas, para asegurar que el procesamiento de la información es el correcto y adecuado

- ◉ SI
- ○ NO aplicable
- ○ NO

12.3 Objetivo — **Controles criptográficos**

Proteger la confidencialidad, privacidad o integridad de la información por medio de la criptografía

12.3.1 — **Política sobre el uso de los controles criptográficos**

Es la gestión del riego usada para determinar cuando es necesario un control criptográfico

- ◉ SI
- ○ NO

Existen políticas que permitan el uso de controles criptográficos para proteger la información

	◉SI ○No requerido ○NO
	Cual de los siguientes elementos no son incluidos cuando se identifica un nivel de protección criptográfico
	☐Tipo/Calidad del algoritmo ☐Longitud de las llaves ☐Restricciones y regulaciones
	Cuando se utilizan las firmas digitales, es apropiado proteger la integridad y confidencialidad de la llave privada
	○SI ○No requerido ◉NO
	Se han tomado en cuenta las consideraciones legales vigentes referentes al uso de las firmas digitales
	○SI ◉NO
	Se han considerado los servicios de no repudio para resolver y dirimir conflictos de la ocurrencia o no de una acción o evento
	◉SI ○No aplicable ○NO
12.3.2	**Administración de llaves**
	Están todas las llaves criptográficas protegidas contra modificación y destrucción
	○ SI ○No aplicable ◉NO
	Es adecuado un sistema de administración de llaves, basado en estándares, procedimientos y métodos seguros
	○SI ◉NO aplicable ○NO
	Las llaves criptográficas tiene definidos fechas de activación y desactivación
	○SI ◉NO aplicable ○NO
	Para las llaves públicas se usa una autoridad de certificación reconocida
	○SI ◉NO aplicable ○NO
12.4	**Seguridad de los sistemas de archivos**
Objetivo	Asegurar la seguridad en los sistemas de archivos
12.4.1	**Control de software operacional**
	Todo software provisto por un proveedor mantiene un nivel adecuado de soporte, y cualquier decisión de actualización toma en cuenta la seguridad de la nueva versión
	○SI ○NO aplicable ◉NO
	Existen controles estrictos sobre la instalación de software en los sistemas operacionales
	◉SI ○NO
	Cual de los siguientes controles no son utilizados para controlar la instalación de software dentro del sistema
	☐Actualización de software por administradores ☐Ejecución únicamente de código ☐Evaluación y evidencia de correcto funcionamiento ☐Registro de actualizaciones de programa y librerías ☐Almacenamiento de versiones anteriores como contingencia ☐Estrategia de roll back ☐Sistema de control de configuraciones
12.4.2	**Protección de los datos de prueba**
	Están protegidos y controlados los datos de pruebas
	○SI ◉No
	Cual de los siguientes controles sobre los datos de prueba no están en uso
	☐Aplicación de los mismo controles de acceso a los datos de prueba ☐Autorización independiente para copias de producción a pruebas ☐Eliminación de los datos en los ambientes de pruebas ☐Registro de auditoria la copia de los datos de producción
12.4.3	**Control de acceso al código fuente del programa**
	Cual de los siguientes elementos no son usados para restringir el acceso a los códigos fuentes de las aplicaciones y librerías
	☐No deben estar sujetos al sistema operacional ☐Acceso restringido para personal de TI ☐Actualizaciones debe ser autorizada ☐Registro de logs de acceso ☐Procedimientos de control de cambios
12.5	**Seguridad en los procesos de desarrollo y soporte**
Objetivo	mantener la seguridad de la información y de las aplicaciones
12.5.1	**Procedimientos de control de cambios**
	Existe un procedimiento de control de cambios que gobierne la implementación de los cambios a los sistemas de información de la organización
	◉SI ○No

Cual de los siguientes elementos no son tenidos en cuenta en el procedimiento de control de cambios

- [ ] Registro de niveles de autorización
- [ ] Cambios realizados únicamente por los usuarios autorizados
- [ ] Revisión de controles e integridad por cambios
- [ ] Identificación de software/hardware que requiera ajustes
- [ ] Aprobación antes de que el trabajo inicie
- [ ] Uso aceptable antes de iniciar
- [ ] Sistema de documentación actualizado
- [ ] Mantener control de versiones
- [ ] Registros de logs de operaciones

12.5.2 **Revisiones técnicas de las aplicaciones despues de cambios en el sistema operativo**

Son los impactos de seguridad de los cambios al sistema operacional sujetos de revisión para validar que los cambios no tengan un efecto adverso sobre la aplicación

- (●) SI
- ( ) No

Cual de los siguientes puntos no es incluido en la revisión de aplicaciones luego de realizar cambios al sistema operacional

- [ ] Control e integridad de las aplicaciones
- [ ] Asignación de tiempo en el plan de pruebas y presupuestos
- [ ] Notificación de los cambios
- [ ] Validar el plan de continuidad

12.5.3 **Restricción en los cambios a los paquetes de software**

El software suministrado externamente es usado sin modificaciones

- (●) SI
- ( ) No hay provedores de software externos
- ( ) NO

Cual de los siguientes puntos no son considerados cuando se necesita modificar un software de un proveedor

- [ ] Riesgo de compromiso del control
- [ ] Permiso del proveedor
- [ ] Obtener cambios del proveedor
- [ ] Responsabilidad por el mantenimiento

12.5.4 **Fuga de información**

En la adquisición de software, son tomadas las medidas adecuadas para minimizar el riesgo de canales encubiertos (cover channels) o software malicioso

- ( ) SI
- (●) No

12.5.5 **Desarrollo de sofwtare externo**

Cual de los siguientes puntos no son considerados cuando el desarrollo del software es entregado a un tercero

- [ ] Derechos de propiedad intelectual, propiedad del código, licenciamiento
- [ ] Certificación de calidad y exactitud del trabajo ejecutado
- [x] Acuerdos de custodia
- [x] Derechos de acceso para realizar auditorias
- [x] Requerimientos legales y contractuales
- [ ] Evaluación antes de poner en funcionamiento

12.6 **Administración técnica de vulnerabilidades**

Objetivo

Reducir el riegos resultante de la explotación de las vulnerabilidades técnicas

12.6.1 **Control de vulnerabildiades técnicas**

Hay un procedimiento establecido para obtener la información sobre las vulnerabilidades técnicas publicadas que existen de los sistemas de información de la organización

- ( ) SI
- (●) No

Cuales de los siguientes elementos no se incluyen en el procedimiento de manejo de vulnerabilidades

- [ ] Roles y Responsabilidades
- [x] Recursos de información
- [x] Definición de líneas de tiempo
- [ ] Valoración del riesgo
- [x] Evaluación de los parches