Universidad Nacional de Costa Rica
Escuela de Informática
Ingeniería en Sistemas de Información
Curso: Administración de Bases de Datos

Valoración del Riesgo de confidencialidad del área de bases de datos de TI

Profesor:
MSc. Johnny Villalobos Murillo

Integrantes:

Adán Rivera Sánchez	114540821
Cesar Cornejo Gómez	115340566
David Ugalde Solís	114180736
Elena Mora Cordero	115530351

Martes 29 de agosto de 2017
Campus Benjamín Núñez, Lagunilla, Heredia, Costa Rica

Contenido

Resumen Ejecutivo

La Ley General de Control Interno establece los criterios mínimos que deben prevalecer para el establecimiento, funcionamiento, mantenimiento, perfeccionamiento y evaluación del sistema de control interno de una entidad, en su artículo 14 expone el componente de la valoración del riesgo, donde se indican los deberes que debe cumplir el jerarca y los titulares subordinados al “identificar y analizar” los riesgos relevantes que afecten los objetivos y metas indicados en los planes de mediano y largo plazo, analizar la probabilidad de ocurrencia y sus posibles efectos y sus medidas de acción para mitigar el riesgo, con el fin de ubicar a la institución en un nivel aceptable.

Como trabajo de estudio y comprensión de los temas a tratar en el curso de administración de bases de datos de la Universidad Nacional de Costa Rica se expone este documento en concordancia al cumplimiento de la ley general de Control Interno (8292) en lo relacionado con la implementación del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) en lo que respecta a riego de confidencialidad en el área de TI para una empresa posteriormente formulada.

Problema

La administración ha evaluado el riesgo de confidencialidad en 12pts (3 impacto, 4 probabilidad de ocurrencia). Se ha sugerido además que dentro de la dirección de TI, las áreas que contribuyen a este riesgo son; Sistemas y Bases de datos, otorgando un responsabilidad de un 50% a cada una.

Objetivo

Elaborar un plan de acción, en el área de Bases de datos del departamento de TI que permita administrar los riesgos que afecten a esta área y las acciones que se daban de poner en práctica para disminuir los riesgos administrativos.

Escala del Nivel de Riesgos

		Rango		
Código	**Descripción**	**Desde**	**Hasta**	**Zona de Riesgo**
1	Bajo	1	2	Verde Claro
2	Medio	3	6	Amarillo
3	Alto	7	14	Naranja
4	Crítico	15	25	Rojo Oscuro

Área de Base de Datos (Riesgo de Confidencialidad)

Tabla Resumen

Apartado	**Factor de Riesgo**	**ISO27002**	**Controles asociados**
DS5 Garantizar la seguridad de los sistemas	**DS5.2** Plan de Seguridad de TI	**5.1** Políticas de seguridad de información	**5.1.1** Documento de política de seguridad de la información (a,b,c,d,e,f)
	DS5.3 Administración de Identidad	**11.2** Administración de acceso a usuario	**11.2.1** Usuario registrado: (a,b,c,d,e,f,g,h,i,j), **11.2.2** Gestión de Privilegios (a,b,c,d,e,f), **11.2.4** Revisión de los derechos de acceso a usuario (a,b,c,d,e)
	DS5.4 Administración de Cuentas del Usuario	**11.2** Administración de acceso a usuario	**11.2.1** Usuario registrado: (a,b,c,d,e,f,g,h,i,j).
	DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad	**10.10** Monitoreo	**10.10.3** Protección de la información de registro. (a,b) **10.10.2 (a,b,c,d,e)**
	DS5.6 Definición de Incidente de Seguridad	**13.1** Reporte de información de eventos de seguridad y vulnerabilidades	**13.1.1** Informes eventos de seguridad de la información (a,b,c,d).

			13.1.2 Informes debilidades de seguridad
	DS5.8 Administración de Llaves Criptográficas	**12.3** Controles Criptográficos	**12.3.1** Política sobre el uso de controles criptográficos (a,b,c,d,e,f,g). **12.3.2** Gestión de claves (a,b,c,d,e,f,g,h,i,j,k).
	DS5.11 Intercambio de Datos Sensitivos	**10.8** Intercambio de Información	**10.8.1** Políticas y procedimientos de intercambio de información (a,b,c,d,e,f,g,h,i,j,k,l,m,n,o). **10.8.2** Los acuerdos de intercambio (a,b,c,d,e,f,g,h,i,j,k).
P09 Evaluar y administrar los Riesgos de TI	**P09.1** Marco de Trabajo de Administración de Riesgos.	**4.2** Tratamiento de los riesgos de seguridad	ver el apartado
	PO9.2 Establecimiento del Contexto del Riesgo.	**4.2** Tratamiento de los riesgos de seguridad	ver el apartado
	PO9.4 Evaluación de Riesgos de TI.	**4.2** Tratamiento de los riesgos de seguridad	ver el apartado
	PO9.5 Respuesta a los Riesgos.	**4.2** Tratamiento de los riesgos de seguridad	ver el apartado
	PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos	**4.2** Tratamiento de los riesgos de seguridad	ver el apartado
P02 Definir la arquitectura de la información	**P02.3** Esquema de clasificación de datos	**5.1** Políticas de seguridad de información	**5.1.1** Documento de política de seguridad de la información (a,b,c,d,e,f).

Entregar y Dar Soporte

DS5 Garantizar la seguridad de los sistemas

DS5.2 Plan de Seguridad de TI

Consiste en trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, el personal, en software y en hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

- *Controles aplicados:*

5.1 Políticas de seguridad de la información

5.1.1 Documento de política de seguridad de información

Documento que debe aprobarse por la gerencia, y ser publicado y comunicado a todo el personal y terceros de importancia de la empresa. El documento debe de contener:

a) Una definición de seguridad de la información, sus objetivos generales, el alcance y la importancia de la seguridad como un mecanismo que permite el intercambio de información (véase la introducción).
b) Una declaración de la intención de la administración, el apoyo a los objetivos y principios de la información de seguridad en línea con la estrategia y los objetivos de negocio.
c) Un marco para ajustar los objetivos de control y los controles, incluyendo la estructura de riesgo, evaluación y gestión de riesgos.
d) Una breve explicación de las políticas de seguridad, los principios, las normas y el cumplimiento requisitos de especial importancia para la organización, incluyendo:
    a. Cumplir con la legislación, reglamentos, y requerimientos contractuales;
    b. Educación de seguridad, formación y sensibilización requisitos;
    c. La gestión de la continuidad del negocio;
    d. Consecuencias de violaciones de política de seguridad de la información;

e) Una definición de las responsabilidades generales y específicas para la gestión de seguridad de la información, incluyendo reportes de incidentes de seguridad de la información.

f) Las referencias a la documentación que puede apoyar la política, la seguridad por ejemplo más detallado políticas y procedimientos para los sistemas de información específicos o normas de seguridad los usuarios deberían cumple con esto.

DS5.3 Administración de Identidad

Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

- *Controles aplicados:*

11.2: Administración de Acceso de Usuario

11.2.1 Usuario registrado

Debe existir una manera formal de registrar usuarios y un procedimiento para eliminarlos, permitir y revocar permisos de acceso a la información.

a) Utilizar ID únicos para cada usuario y ver a los responsables de cada acción; el uso de identificadores de grupo sólo se autorizará cuando sean necesarias para razones de negocios o de funcionamiento, y deben ser aprobados y documentados.
b) Comprobar que el usuario tiene autorización para el uso del sistema de información o servicios; la aprobación por separado de los derechos de acceso de la administración también puede ser apropiado.
c) Comprobar que el nivel de acceso concedido es adecuado al propósito de negocios y es coherente con la política de seguridad de la organización.
d) Dar a los usuarios una declaración escrita de sus derechos de acceso.
e) Los usuarios deben firmar declaraciones que indican que entiendan las condiciones de acceso.
f) La garantía de los proveedores de servicios no proporcionan el acceso hasta que los procedimientos de autorización han sido completados.

g) Mantener un registro formal de todas las personas registradas para usar el servicio.
h) Eliminar de inmediato o bloquear los derechos de acceso a los usuarios que han cambiado los roles o puestos de trabajo o han sido despedidos de la organización.
i) Comprobación periódica de los ID de usuario despedidos y eliminación o bloqueo, de sus cuentas.

j) Asegurar que los ID de usuarios despedidos no se emiten a otros usuarios.

11.2.2 Gestión de privilegios

La asignación y uso de los privilegios debe ser restringido y controlados.

a) Los privilegios de acceso asociados a cada producto del sistema, por ejemplo, sistema operativo, base de datos, sistema de gestión y cada aplicación, los usuarios a los que tienen que estar asignado debe ser identificado.
b) Los privilegios deben asignarse a los usuarios con base a la necesidad de uso y en un “evento por evento” base de acuerdo con la política de control de acceso (11.1.1), es decir, el requisito mínimo para su papel funcional sólo cuando sea necesario.
c) Deben mantenerse un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben concederse hasta que el proceso de autorización es completado.
d) El desarrollo y uso de las rutinas del sistema deben promoverse para evitar la necesidad de conceder privilegios a los usuarios.
e) El desarrollo y la utilización de programas, que evitan la necesidad de ejecutar con privilegios deberían ser promovido.
f) Los privilegios deben ser asignados a un ID de usuario diferentes de los utilizados para los negocios de uso normal.

11.2.4 Revisión de los derechos de acceso de usuario

La Gerencia debe comprobar el acceso correcto, periódicamente usando un proceso formal.

a) Los derechos de acceso de los usuarios deben ser revisados periódicamente, por ejemplo, un período de 6 meses, después de cualquier cambio, como la promoción, degradación o despido (véase 11.2.1).
b) Los derechos de acceso de usuario deben ser revisados y re-asignados al cambiar en la empresa.

c) Las autorizaciones de los derechos especiales de acceso privilegiado (ver 11.2.2) deben ser revisados en intervalos de tiempo más frecuentes, por ejemplo, en un período de 3 meses.
d) Las asignaciones de privilegios deben ser revisados en intervalos de tiempo regulares para asegurar que no se han obtenido privilegios inadecuados.
e) Los cambios en las cuentas privilegiadas deben ser registrados para su revisión periódica.

DS5.4 Administración de Cuentas del Usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

- *Controles aplicados:*

11.2: Administración de acceso a usuarios

11.2.1 Usuario registrado

Debe existir una manera formal de registrar usuarios y un procedimiento para eliminar usuarios, permitir y revocar permisos de acceso a la información.

a) Utilizar ID únicos para cada usuario y ver a los responsables de cada acción; el uso de identificadores de grupo sólo se autorizará cuando sean necesarias para razones de negocios o de funcionamiento, y deben ser aprobados y documentados.
b) Comprobar que el usuario tiene autorización para el uso del sistema de información o servicio; aprobación por separado de los derechos de acceso de la administración también puede ser apropiado.
c) Comprobar que el nivel de acceso concedido es adecuada al propósito de negocios (véase 11.1) y es coherente con la política de seguridad de la organización, por ejemplo, no hace compromiso separación de funciones (véase 10.1.3).
d) Dar a los usuarios una declaración escrita de sus derechos de acceso.

e) Que usuarios tengan que firmar declaraciones que indican que entiendan las condiciones de acceso.
f) La garantía de los proveedores de servicios no proporcionan el acceso hasta que los procedimientos de autorización han sido completados.
g) Mantener un registro formal de todas las personas registradas para usar el servicio.
h) Eliminar de inmediato o bloquear los derechos de acceso a los usuarios que han cambiado los roles o puestos de trabajo o han sido despedidos de la organización.
i) Comprobación periódica de los ID de usuario despedidos y eliminación o bloqueo, de sus cuentas.

j) Asegurar que los ID de usuarios despedidos no se emiten a otros usuarios.

DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad

Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser re-acreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

- *Controles aplicados:*

10.10: Monitoreo

10.10.2 Uso Sistema de seguimiento

Procedimientos para el uso de vigilancia de las instalaciones de procesamiento de información deben ser establecidas y los resultados de las actividades de seguimiento de revisiones regulares.

a) El acceso autorizado, incluyendo detalles, tales como:
   1) El ID de usuario;
   2) La fecha y hora de los eventos clave;
   3) Los tipos de eventos;
   4) Los archivos tiene acceso;
   5) El programa / utilidades utilizados;

b) Todas las operaciones privilegiados, tales como:
   1) El uso de cuentas privilegiadas, por ejemplo supervisor, raíz, administrador;
   2) Sistema de puesta en marcha y parada;
   3) I / O de fijación de dispositivo / desprendimiento;

c) Los intentos de acceso no autorizados, tales como:
   1) Fallado o rechazado las acciones del usuario;
   2) Fallado o rechazada acciones que involucran datos y otros recursos;
   3) Violaciones de política de acceso y notificaciones para puertas de enlace y servidores de seguridad de red;
   4) Alertas de los sistemas de detección de intrusión de propiedad;

d) Alertas del sistema o fallas como:
   1) Alertas o mensajes de consola;
   2) Excepciones de registro del sistema;
   3) Alarmas de gestión de red;
   4) Alarmas planteadas por el sistema de control de acceso;

e) Los cambios o intentos realizados en la configuración de seguridad del sistema, o en los controles deben revisarse periódicamente; los resultados de las actividades de monitoreo deben depender de los riesgos involucrados. Entre los factores de riesgo que deben ser considerados incluyen:
   1) Criticidad de los procesos de aplicación.
   2) El valor, la sensibilidad, y la criticidad de la información en cuestión.
   3) Los reportes sobre la experiencia de la infiltración del sistema, la frecuencia de las vulnerabilidades, y su mal uso deben ser explotados.
   4) Extensión de la interconexión del sistema (en particular las redes públicas);
   5) Se desactiva función de registro.

10.10.3 Protección de la información de registro

Las instalaciones de registro y la información de registro deben estar protegidas contra la manipulación y el acceso no autorizado, entre los cuales están los siguientes.

a) Las modificaciones de los tipos de mensaje que se registran.
b) Los archivos de registro de ser editados o eliminados.
c) Capacidad de almacenamiento del medio de archivo de registro que se excede, resultado de la Grabación de los eventos o sobrescritos de eventos anteriormente grabados.

DS5.6 Definición de Incidente de Seguridad

Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.

- *Controles aplicados:*

13.1: Reporte de información de eventos de seguridad y vulnerabilidades

13.1.1 Informes eventos de seguridad de la información

Los eventos de la seguridad de la información deberá ser reportada mediante canales administrativos apropiados, rápidos si es posible.

a) Los procesos adecuados de retroalimentación para asegurar que aquellos que informaron eventos sobre la seguridad de la información sean notificados de los resultados después de que el tema haya sido tratado y cerrado.

b) Bitácora de incidentes sobre la seguridad de la información que posea acciones y descripción del evento, que sirva de ayuda en futuros eventos sobre la seguridad de la información

c) El correcto comportamiento a ejecutar en caso de un evento seguridad de la información, es:
   1) Observar todos los detalles importantes (por ejemplo, tipo de incumplimiento o incumplimiento, ocurriendo mal funcionamiento, los mensajes en la pantalla, comportamiento extraño) inmediatamente.
   2) No llevar a cabo ninguna acción propia, pero informar inmediatamente encargado.

d) Referenciar el proceso disciplinario establecido por el negocio para tratar con los empleados, contratistas o terceros usuarios que cometen infracciones de seguridad.

13.1.2 Informes debilidades de seguridad

Todos los empleados, contratistas y terceros usuarios del sistema de información y servicios deberán tomar nota y reportar cualquiera observación o sospecha de debilidad de seguridad en los sistemas o servicios.

DS5.8 Administración de Llaves Criptográficas

Determinar que las políticas y procedimientos para organizar la generación, modificación, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas esté implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

- *<u>Controles aplicados:</u>*

12.3: Política sobre el uso de controles criptográficos:

12.3.1 Política sobre el uso de controles criptográficos

Elaborar una política sobre el uso de los controles criptográficos para la protección de la información e implementado.

a) El enfoque de gestión hacia el uso de los controles criptográficos en la organización, incluidos los principios generales en las que la información comercial debe ser protegida (véase también 5.1.1).
b) Basado en la evaluación de riesgos, el nivel requerido de protección debe ser identificado teniendo en cuenta el tipo, la fuerza, y la calidad del algoritmo de cifrado requerida.
c) El uso de cifrado para la protección de la información sensible transportada por el móvil o medios extraíbles, dispositivos o a través de líneas de comunicación.
d) El enfoque de la gestión de claves, incluyendo métodos para hacer frente a la protección de claves criptográficas y la recuperación de la información codificada en el caso de pérdida, comprometido o daño de claves.
e) Las funciones y responsabilidades, por ejemplo, quién es responsable de:
   1) la aplicación de la política.
   2) la gestión de claves, incluyendo la generación de claves (ver también 12.3.2).
f) Las normas que deben adoptarse para la aplicación efectiva en toda la organización (Que solución se utiliza para que los procesos de negocio).
g) El impacto del uso de la información encriptada sobre los controles que dependen de la inspección de contenido (Por ejemplo la detección de virus).

12.3.2 Gestión de claves

Administración de claves debe ser la adecuada, para apoyar el uso de las técnicas de criptografía en las organizaciones.

a) La generación de claves para los diferentes sistemas criptográficos y diferentes aplicaciones.
b) Generar y obtener certificados de clave pública.
c) Distribuir claves a los usuarios previstos, incluida la forma claves deben ser activados cuando recibido;
d) Almacenar claves, incluyendo cómo los usuarios autorizados obtengan acceso a las claves;

e) Cambiar o actualizar las claves incluidas las normas sobre cuando las claves se deben cambiar y cómo se hará;
f) Reglamento sobre las claves comprometidas;
g) Revocar claves incluyendo cómo deben ser retirados o desactivados, cuando las llaves, se han comprometido o un usuario deja la organización (en el que las claves caso debe también ser archivados).
h) Recuperar las llaves que se pierden o corrompen como parte de la continua administración del negocio, por ejemplo, para la recuperación de la información cifrada.
i) Registro de las llaves, por ejemplo para información de archivado o la copia de seguridad;
j) La destrucción de llaves;
k) registro y la auditoría de la administración relacionada a las actividades de las llaves.

DS5.11 Intercambio de Datos Sensitivos

Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

- *Controles aplicados:*

10.8: Intercambio de Información

10.8.1 políticas y procedimientos de intercambio de información

Políticas formales de intercambio, procedimientos y controles que deben estar para proteger el intercambio de información mediante el uso de todo tipo de medios de comunicación.

a) Los procedimientos diseñados para proteger la intercepción de la información intercambiada, copiado, modificación, y la destrucción;
b) Los procedimientos para la detección y la protección contra código malicioso que puede ser transmitida a través del uso de las comunicaciones electrónicas (véase la cláusula 10.4.1).
c) Procedimientos para proteger comunicación electrónica con información sensible que está en forma de un archivo adjunto;
d) La política o directrices que describen el uso aceptable de medios electrónicos de comunicación (ver 7.1.3).
e) Procedimientos para el uso de las comunicaciones inalámbricas, teniendo en cuenta los riesgos particulares involucrados.

f) Los empleados, contratistas y cualquier otro usuario tienen la responsabilidad de no comprometer a la organización, por ejemplo, a través de la difamación, acoso, suplantación, el reenvío de información, compras no autorizadas, etc.

g) El uso de técnicas criptográficas, por ejemplo, para proteger la confidencialidad, la integridad y autenticidad de la información (véase el numeral 12.3).

h) Retención y directrices para la eliminación de toda la correspondencia comercial, incluidos los mensajes, en conformidad con la legislación y los reglamentos nacionales y locales pertinentes.

i) No dejar información sensible o crítica en instalaciones de impresión, por ejemplo fotocopiadoras, impresoras y fax, ya que estos pueden ser accedidos por personal no autorizado.

j) Controles y restricciones asociadas con la transmisión de medios de comunicación, por ejemplo, el reenvío automático de correo electrónico a direcciones de correo electrónico externas.

k) Recordando al personal que deben tomar las precauciones apropiadas, por ejemplo, para no revelar información sensible para evitar ser escuchados o interceptado al hacer una llamada telefónica por:

1) Las personas en su vecindad inmediata, particularmente cuando se usan los teléfonos móviles.
2) Las intervenciones telefónicas, y otras formas de espionaje ilegales a través del acceso físico al auricular del teléfono o la línea de teléfono, o el uso de receptores de exploración.
3) Personas al final del destinatario.

l) No dejar mensajes que contengan información sensible en las máquinas contestadoras ya que éstas pueden ser reproducidas por personas no autorizadas, almacenadas en sistemas comunales o almacenados incorrectamente como resultado de una mala señalización.

m) Recordando al personal sobre los problemas del uso de máquinas de fax, a saber:

1) Acceso no autorizado a los almacenes de mensajes incorporados para recuperar mensajes.
2) Programación deliberada o accidental de las máquinas para enviar mensajes a números en específico.
3) Envío de documentos y mensajes a un número, ya sea por marcar de forma equivocada o el uso el número almacenado incorrecto.

n) Recordando al personal que no registre datos demográficos, como la dirección de correo electrónico u otra información personal, en cualquier software para evitar la recopilación para uso no autorizado.

o) Recordando al personal que las máquinas de fax modernas y las fotocopiadoras tienen cachés de páginas y almacenan páginas en caso de un fallo, que se imprimirá una vez que se haya eliminado la falla.

10.8.2 Los acuerdos de intercambio

Deberían establecerse acuerdos para el intercambio de información y software entre la organización y las partes externas

a) Las responsabilidades de gestión para controlar y notificar la transmisión, despacho, y recibo.
b) Procedimientos para notificar el remitente de la transmisión, despacho y la recepción.
c) Procedimientos para garantizar la trazabilidad y el no repudio.
d) Normas técnicas mínimas para el embalaje y la transmisión.
e) Acuerdos de fideicomiso.
f) Estándares de identificación del correo.
g) Las responsabilidades y obligaciones en caso de incidentes de seguridad de la información, como la pérdida de datos.
h) El uso de un sistema de etiquetado acordado para la información sensible o crítica, asegurándose que el significado de las etiquetas se entendido inmediatamente y que la información es apropiadamente protegida.
i) La propiedad y las responsabilidades para la protección de datos, derechos de autor, el cumplimiento de licencias de software y consideraciones similares.
j) Estándares técnicos para el registro de la información y software.
k) Cualquier control especial que puede ser necesario para proteger elementos sensibles, tales como criptográfica.

Planeación y Organización

P09 Evaluar y administrar los riesgos de TI

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.

PO9.1 Marco de Trabajo de Administración de Riesgos

Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.

PO9.2 Establecimiento del Contexto del Riesgo

Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.4 Evaluación de Riesgos de TI

Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

PO9.5 Respuesta a los Riesgos

Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos

Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

- *Controles aplicados para PO9.1,PO2,P04,PO5,PO6 :*

4.2 El tratamiento de los riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, la organización debe definir criterios para determinar si los riesgos están en un rango aceptable o no. Los riesgos pueden ser aceptables si, por ejemplo, se considera que el riesgo es bajo o que el coste de tratamiento no es rentable para la organización. Tales decisiones deben ser grabadas.

Para cada uno de los riesgos identificados a raíz de la evaluación del riesgo de una decisión de tratamiento del riesgo tiene que ser realizado. Las posibles opciones para el tratamiento del riesgo incluyen:

a) Aplicar controles apropiados para reducir los riesgos.

b) Aceptar a sabiendas y objetivamente riesgos, siempre que satisfagan claramente la política y los criterios de aceptación del riesgo de la organización.

c) Evitar riesgos al no permitir acciones que causarían los riesgos de que se produzca.

d) La transferencia de los riesgos asociados a otras partes, por ejemplo, los aseguradores o proveedores.

En los riesgos en que la decisión del tratamiento del riesgo ha sido aplicar los controles adecuados, estos controles deben seleccionarse e implementarse para cumplir con los requisitos identificados por una evaluación de riesgos.

Los Controles deben asegurar que los riesgos se reducen a un nivel aceptable teniendo en cuenta lo siguiente:

a) Los requisitos y limitaciones de la legislación y la normativa nacional e internacional.

b) Objetivos de la organización.

c) Requisitos y restricciones operacionales.

P02 Definir la arquitectura de la información

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio.

Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.

PO2.3 Esquema de Clasificación de Datos

Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son.
Se usa como base para aplicar controles como el control de acceso, archivo o cifrado.

- *Controles aplicados:*

5.1 Políticas de seguridad de la información (ISO27002)

5.1.1 Documento de políticas de seguridad de información

Documento que debe aprobarse por la gerencia, y ser publicado y comunicado a todo el personal y terceros de importancia de la empresa, este documento debe de contener:

a) Una definición de seguridad de la información, sus objetivos generales, el alcance y la importancia de la seguridad como un mecanismo que permite el intercambio de información.
b) Una declaración de la intención de la administración, el apoyo a los objetivos y principios de la información de seguridad en línea con la estrategia y los objetivos de negocio.
c) Un marco para ajustar los objetivos de control y los controles, incluyendo la estructura de riesgo, evaluación y gestión de riesgos.
d) Una breve explicación de las políticas de seguridad, los principios, las normas y el cumplimiento requisitos de especial importancia para la organización, incluyendo:

1. Cumplir con la legislación, reglamentos, y requerimientos contractuales;
2. Educación de seguridad, formación y sensibilización requisitos;
3. La gestión de la continuidad del negocio;
4. Consecuencias de violaciones de política de seguridad de la información;

e) Una definición de las responsabilidades generales y específicas para la gestión de seguridad de la información, incluyendo reportes de incidentes de seguridad de la información.
f) Las referencias a la documentación que puede apoyar la política, la seguridad por ejemplo más detallado políticas y procedimientos para los sistemas de información específicos o normas de seguridad los usuarios deberían cumple con esto.

Referencias

(n.d.). Retrieved 08 2017, from http://www.iso27000.es/download/ControlesISO27002-2005.pdf

ISO/IEC 27002 INTERNATIONAL STANDARD. (2005, 06 15). Retrieved 08 2017, from http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf

IT Governance Institute. (n.d.). *COBIT 4.1.* Retrieved 08 2017, from http://www.isaca.org/knowledge-center/cobit/documents/cobit4.pdf