NORMA TÉCNICA PERUANA

NTP-ISO/IEC 27005
2018

Dirección de Normalización - INACAL
Calle Las Camelias 817, San Isidro (Lima 27)

Lima, Perú

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información

Information technology. Security techniques. Information security risk management

(EQV. ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management)

2018-12-28
2ª Edición

R.D. N° 047-2018-INACAL/DN. Publicada el 2019-01-16

Precio basado en 91 páginas

I.C.S.: 03.100.70; 35.030

ESTA NORMA ES RECOMENDABLE

Descriptores: Tecnología de la información, técnica de seguridad, gestión de riesgo, tecnología, información, seguridad, gestión

© ISO/IEC 2018 - © INACAL 2018

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018

Todos los derechos son reservados. A menos que se especifique lo contrario, ninguna parte de esta publicación podrá ser reproducida o utilizada por cualquier medio, electrónico o mecánico, incluyendo fotocopia o publicándolo en el Internet o intranet, sin permiso por escrito del INACAL, único representante de la ISO/IEC en territorio peruano.

© INACAL 2018

Todos los derechos son reservados. A menos que se especifique lo contrario, ninguna parte de esta publicación podrá ser reproducida o utilizada por cualquier medio, electrónico o mecánico, incluyendo fotocopia o publicándolo en el internet o intranet, sin permiso por escrito del INACAL.

INACAL

Calle Las Camelias 817, San Isidro
Lima - Perú
Tel.: +51 1 640-8820
administracion@inacal.gob.pe
www.inacal.gob.pe

ÍNDICE

página

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PRÓLOGO

A. RESEÑA HISTÓRICA

A.1 El Instituto Nacional de Calidad - INACAL, a través de la Dirección de Normalización es la autoridad competente que aprueba las Normas Técnicas Peruanas a nivel nacional. Es miembro de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), en representación del país.

A.2 La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de julio a setiembre de 2018, utilizando como antecedente a la norma ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management.

A.3 El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos presentó a la Dirección de Normalización -DN-, con fecha 2018-10-02, el PNTP-ISO/IEC 27005:2018, para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2018-10-19. No habiéndose recibido observaciones, fue oficializada como Norma Técnica Peruana **NTP-ISO/IEC 27005:2018 Tecnología de la información. Técnicas de seguridad. Gestión de riesgo de la seguridad de la información**, 2ª Edición, el 16 de enero de 2019.

A.4 Esta segunda edición de la NTP-ISO/IEC 27005 reemplaza a la NTP-ISO/IEC 27005:2009 EDI. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:2016 y GP 002:2016.

B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACIÓN DE LA NORMA TÉCNICA PERUANA

Secretaría	GS1 PERU
Presidente	Ricardo Dioses

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Secretaria	Mary Wong

ENTIDAD	**REPRESENTANTE**
Contraloría General de la República	Joel Enrique Mercado Rojas Marco Antonio Bermúdez Torres
Deloitte & Touche S. R. L.	Diana Lagos Flores Pedro Alberto Torres Fuentes
DMS Perú S. A. C.	Adela Barcenas
GS1 PERÚ	Marita Hernández Milagros Davila
IBM del Perú S. A. C.	Alann Reyes Ivan Ancco Peña
Indecopi - Gerencia de Planeamiento y Gestión Institucional	César Augusto Guerra Camargo
International Analytical Services S. A. C. – NSF INASSA S. A. C.	Raúl Miranda Mercado Karla Leon Moran
ITS Consultans S. A. C. (Ahora trabaja en el Consejo Nacional de la Magistratura)	Ricardo Dioses Villanueva
ITSTK Perú S. A. C.	Belén Alvarado Chau Cristhian Meza Cortez
Microsoft Perú S. R. L.	Fernando Gebara Filho Héctor Figari Costa
Ministerio de Economía y Finanzas – Oficina de Normalización Previsional – ONP	Jennifer Jacinta Ayllón Bulnes
SUNAT	Jorge Daniel Llanos
Consultor	Carlos A. Horna Vallejos

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PRÓLOGO
(ISO)

ISO (la Organización Internacional de Normalización) e IEC (el International Electrotechnical comisión) forman el sistema especializado para la estandarización mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar campos específicos de actividad técnica. Los comités técnicos de ISO y IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también participan en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1 .

Los procedimientos utilizados para desarrollar este documento y los destinados a su mantenimiento adicional se describen en las Directivas ISO/IEC, Parte 1. En particular, deben tenerse en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documentos. Este documento se redactó de acuerdo con las reglas editoriales de las Directivas ISO/IEC, Parte 2 (consulte www.iso.org/directivas).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO e IEC no serán responsables de la identificación de cualquiera o todos los derechos de patente. Los detalles de cualquier derecho de patente identificado durante el desarrollo del documento estarán en la Introducción y/o en la lista ISO de declaraciones de patentes recibidas (consulte www.iso.org/patentes).

Cualquier nombre comercial utilizado en este documento es información que se proporciona para la comodidad de los usuarios y no constituye un aval.

Para obtener una explicación sobre la naturaleza voluntaria de las normas, el significado de los términos y expresiones específicos de ISO relacionados con la evaluación de la conformidad, así como información sobre la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) en los Obstáculos Técnicos al Comercio (OTC), consulte siguiente URL: www.iso.org/iso/foreword.html .

Este documento fue preparado por el Comité Técnico ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad de TI.

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Cualquier comentario o pregunta sobre este documento debe dirigirse al organismo nacional de estándares del usuario. Se puede encontrar una lista completa de estos cuerpos en www.iso.org/members.html .

Esta tercera edición cancela y reemplaza la segunda edición (ISO/IEC 27005:2011) que ha sido revisada técnicamente. Los principales cambios respecto a la edición anterior son los siguientes:

- todas las referencias directas a ISO/IEC 27001:2005 han sido eliminadas;
- se ha agregado información clara de que este documento no contiene una guía directa sobre la implementación de los requisitos del SGSI especificados en ISO/IEC 27001 (vea Introducción);
- ISO/IEC 27001:2005 se ha eliminado de la capítulo 2;
- ISO/IEC 27001 se ha agregado a la bibliografía;
- el Anexo G y todas sus referencias han sido eliminados; y
- se han realizado cambios editoriales en consecuencia.

PROHIBIDA SU REPRODUCCIÓN

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

INTRODUCCIÓN

Esta Norma Técnica Peruana proporciona directrices para la gestión del riesgo de seguridad de la información en una organización. Sin embargo, esta Norma Técnica Peruana no proporciona ningún método específico para la gestión del riesgo de seguridad de la información. Es la organización la que deberá definir su enfoque para la gestión del riesgo, dependiendo, por ejemplo, del alcance de un sistema de gestión de seguridad de la información (SGSI), del contexto de gestión del riesgo o del sector industrial. Pueden utilizarse un número de metodologías existentes bajo el marco de referencia descrito en esta Norma Técnica Peruana para implementar los requisitos de un SGSI. Esta Norma Técnica Peruana está basado el método basado en activos, amenazas y vulnerabilidades para la identificación de riesgos, que ya no es un requisito de ISO/IEC 27001 . Existen otros enfoques que pueden ser utilizados.

Esta Norma Técnica Peruana no contiene una guía directa sobre la implementación de los requisitos provistos en ISO/IEC 27001 .

Esta Norma Técnica Peruana es relevante para los directores y para el personal vinculado a la gestión del riesgo de seguridad de la información dentro de una organización y, donde sea apropiado, para las partes externas que apoyan sus actividades.

---oooOooo---

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Tecnología de la información. Técnicas de seguridad. Gestión de riesgo de la seguridad de la información

1 Alcance

Esta Norma Técnica Peruana proporciona directrices para la gestión del riesgo de seguridad de la información.

Esta Norma Técnica Peruana apoya los conceptos generales especificados en ISO/IEC 27001 y está diseñado para ayudar en la implementación satisfactoria de seguridad de la información basada en un enfoque de gestión de riesgos.

El conocimiento de los conceptos, modelos, procesos y terminología descritos en ISO/IEC 27001 e ISO/IEC 27002 es importante para un entendimiento completo de este documento.

Esta Norma Técnica Peruana es aplicable a organizaciones de todo tipo (es decir, empresas comerciales, organismos gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

2 Referencias normativas

Los siguientes documentos, se referencian en el texto de tal manera que algunos o todos sus contenidos constituyen requisitos de este documento. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la edición más reciente del documento referenciado (incluida cualquier enmienda).

ISO/IEC 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

3 Términos y definiciones

Para los propósitos de este documento, se aplican los términos y definiciones proporcionadas en la norma ISO/IEC 27000 y los siguientes:

ISO e IEC mantienen bases de datos terminológicas para su uso en la normalización en las siguientes direcciones:

- Plataforma de navegación en línea de ISO: disponible en http://www.iso.org/obp
- IEC Electropedia: disponible en http://www.electropedia.org/

4 Estructura de este documento

Esta Norma Técnica Peruana contiene la descripción del proceso de gestión del riesgo de seguridad de la información y sus actividades.

La información de antecedentes (background) se proporciona en el capítulo 5 .

Una descripción general del proceso de gestión del riesgo de seguridad de la información es presentada en el capítulo 6 .

Todas las actividades de la gestión del riesgo de seguridad de la información son presentadas en el capítulo 6 y posteriormente descritas en los siguientes capítulos:

- establecimiento del contexto en el capítulo 7 ;
- evaluación (assessment) del riesgo en el capítulo 8 ;
- tratamiento del riesgo en el capítulo 9 ;

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- aceptación del riesgo en el capítulo 10 ;
- comunicación del riesgo en el capítulo 11 ; y
- seguimiento (monitoring) y revisión del riesgo en el capítulo 12 .

Información adicional para las actividades de gestión del riesgo de seguridad de la información se presenta en los anexos. El establecimiento del contexto es apoyado por el Anexo A (Definiendo el alcance y los límites del proceso de gestión del riesgo de seguridad de la información). La identificación y evaluación de activos y las valoraciones de impacto se discuten en el Anexo B. El Anexo C proporciona ejemplos de amenazas típicas y el Anexo D discute las vulnerabilidades y los métodos de evaluación de vulnerabilidades. En el Anexo E se presentan ejemplos de enfoques sobre la evaluación del riesgo de seguridad de la información.

Las restricciones para la reducción del riesgo se presentan en el Anexo F .

Todas las actividades de gestión del riesgo presentadas desde el capítulo 7 hasta el capítulo 12 se estructuran como sigue:

Entrada: Identifica cualquier información requerida para realizar la actividad.

Acción: Describe la actividad.

Guía de implementación: Proporciona una guía para la ejecución de la acción. Algunas de estas guías pueden no ser convenientes en todos los casos con lo cual, pueden ser más apropiadas otras maneras de realizar la acción.

Salida: Identifica cualquier información derivada después de realizar la actividad.

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

5 Antecedentes (Background)

Es necesario un enfoque sistemático hacia la gestión del riesgo de seguridad de la información, a fin de identificar necesidades de la organización con respecto a sus requisitos de seguridad de la información y crear un sistema de gestión de la seguridad de la información (SGSI) eficaz. se debería que este enfoque sea adecuado para el entorno de la organización, y en particular se debería alinear con la gestión global del riesgo de la empresa. Los esfuerzos de seguridad deberían tratar los riesgos de una manera eficaz y oportuna donde y cuando sean necesarios. La gestión del riesgo de seguridad de la información debería ser parte integral de todas las actividades de gestión de la seguridad de la información y debería aplicarse tanto en la implantación como en la operación en curso de un SGSI.

La gestión del riesgo de seguridad de la información debería ser un proceso continuo. El proceso debería establecer el contexto interno y externo, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento del riesgo para implementar las recomendaciones y las decisiones. La gestión del riesgo analiza qué puede suceder y cuáles pueden ser las consecuencias posibles, antes de decidir qué debería ser hecho y cuándo, para reducir el riesgo a un nivel aceptable.

La gestión del riesgo de seguridad de la información debería contribuir a:

- que sean identificados los riesgos;
- que sean evaluados los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia;
- que sean comunicadas y entendidas la probabilidad de ocurrencia y las consecuencias de estos riesgos;
- que sea establecido un orden de prioridad para el tratamiento de riesgos;
- que sea establecido un orden de prioridad para acciones que reduzcan riesgos existentes;
- que sean mantenidas informadas las partes interesadas (stakeholders) que estén implicadas, cuando se toman decisiones de gestión del riesgo y sobre el estado de la gestión de riesgos;

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- la efectividad del seguimiento (monitoring) del tratamiento de riesgos;
- el seguimiento y revisión regular de los riesgos y del proceso de gestión del riesgo;
- que sea capturada información para mejorar enfoque de la gestión del riesgo; y
- que sean formados directores y personal sobre los riesgos y sobre las acciones tomados para mitigarlos.

El proceso de gestión del riesgo de seguridad de la información puede ser aplicado a la organización en su totalidad, a cualquier parte de la organización (por ejemplo, un departamento, una localización física, un servicio), a cualquier sistema de información, existente o planeado o a aspectos particulares de control (por ejemplo, planificación de la continuidad del negocio).

6 Descripción del proceso de gestión del riesgo de seguridad de la información

En la norma ISO 31000 y en la Figura 1 se especifica una vista de alto nivel del proceso de gestión del riesgo.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

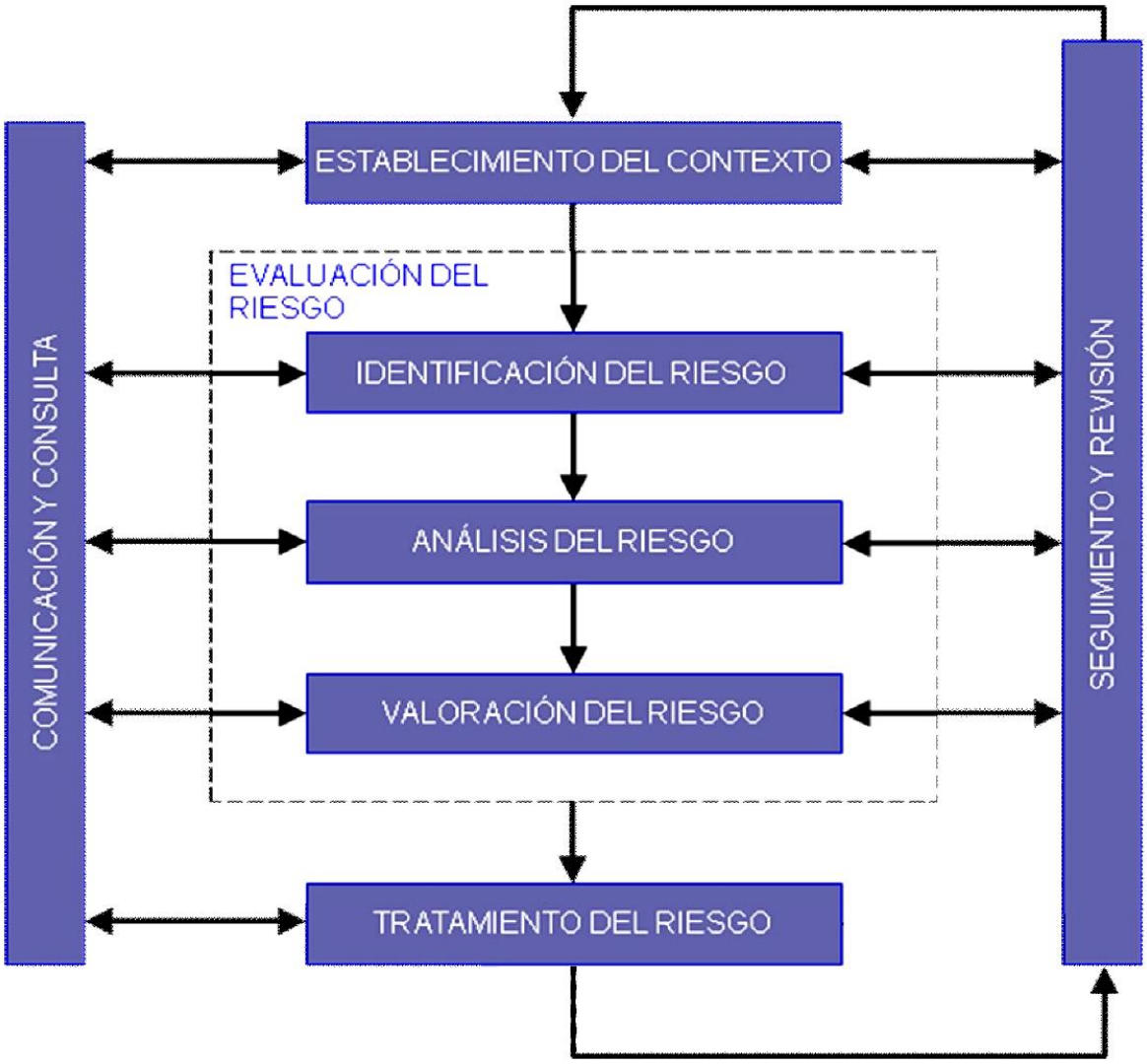

Figura 1 - El proceso de gestión de riesgo

La Figura 2 muestra cómo esta norma aplica este proceso de gestión del riesgo.

El proceso de gestión del riesgo de seguridad de la información consiste en el establecimiento del contexto (capítulo 7), la evaluación del riesgo (capítulo 8), el tratamiento del riesgo (capítulo 9), la aceptación del riesgo (capítulo10), la comunicación y consulta del riesgo (capítulo 11), y el seguimiento y la revisión del riesgo (capítulo 12).

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

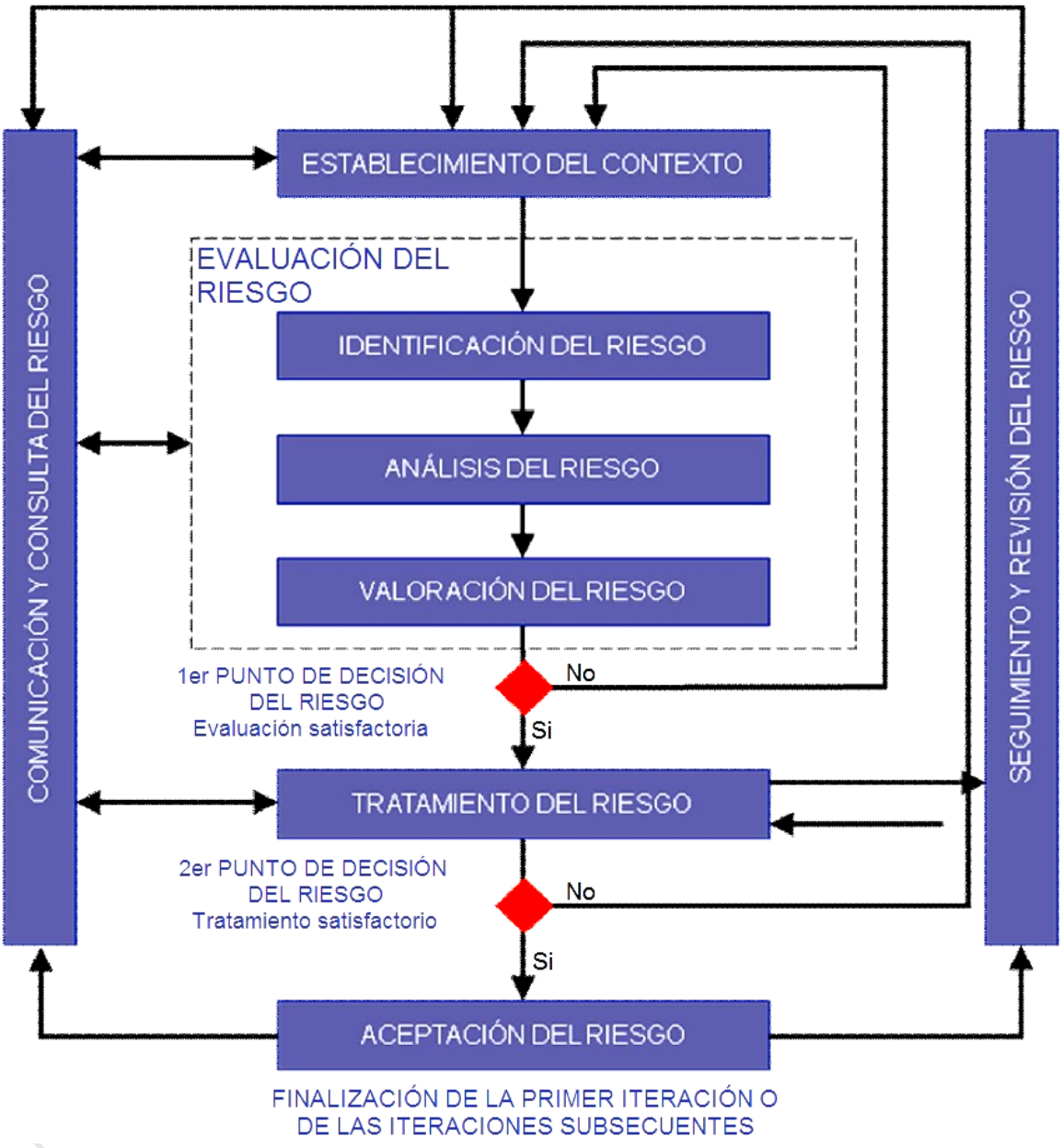

Figura2 – Ilustración de un proceso de gestión del riesgo de seguridad de la información

Como se muestra en la Figura 2, el proceso de gestión del riesgo de seguridad de la información puede ser iterativo para las actividades de valoración y/o tratamiento de riesgos. Un enfoque iterativo para conducir la evaluación del riesgo puede aumentar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo proporciona un buen equilibrio entre minimizar el tiempo y el esfuerzo empleados en

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

identificar controles, mientras que se asegura que los riesgos altos están evaluados apropiadamente.

Primero se establece el contexto. Luego se conduce una evaluación de riesgos. Si esto proporciona la información suficiente para determinar con eficacia las acciones requeridas para modificar los riesgos a un nivel aceptable, entonces la tarea estará completa y se continúa con el tratamiento de riesgos. Si la información es insuficiente, será conducida otra iteración de la evaluación del riesgo con el contexto revisado (por ejemplo, criterios de valoración de riesgos, criterios de aceptación del riesgo o criterios de valoración del impacto), posiblemente en partes acotadas del alcance total (véase la Figura 2, punto de decisión de riesgos 1).

La eficacia del tratamiento del riesgo depende de los resultados de la evaluación de riesgos.

Notar que el tratamiento del riesgo involucra un proceso cíclico de:

- evaluar un tratamiento del riesgo;
- decidir si los niveles de riesgo residual son aceptables;
- generar un nuevo tratamiento del riesgo si los niveles de riesgo no son aceptables; y
- evaluar la eficacia del tratamiento.

Es posible que el tratamiento del riesgo no conduzca inmediatamente a un nivel de riesgo residual aceptable. En esta situación, de ser necesario, puede ser requerida otra iteración de la evaluación del riesgo con los parámetros de contexto modificados (por ejemplo, criterios de evaluación de riesgos, criterios de aceptación del riesgo o criterios de evaluación del impacto), seguido por un tratamiento del riesgo complementario (véase la Figura 2, punto de decisión de riesgos 2).

La actividad de aceptación del riesgo tiene que asegurar que los riesgos residuales son aceptados explícitamente por los directores de la organización. Esto es especialmente importante en una situación donde la implantación de controles se omite o se pospone, por ejemplo, debido al costo.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Durante el proceso global de gestión del riesgo de seguridad de la información es importante que los riesgos y su tratamiento sean comunicados a los directores apropiados y al personal operacional. Incluso antes del tratamiento de los riesgos, la información sobre los riesgos identificados puede tener mucho valor para la gestión de incidentes y puede ayudar a reducir el daño potencial. La concientización de directores y del personal acerca de los riesgos, la naturaleza de los controles implementados para mitigarlos y las áreas que motiven preocupación a la organización, ayuda en el tratamiento de incidentes y eventos inesperados en forma más efectiva. se debería documentar los resultados detallados de cada actividad del proceso de gestión del riesgo de seguridad de la información y de los dos puntos de decisión del riesgo.

ISO/IEC 27001 especifica que los controles implementados dentro del alcance, sus límites y el contexto del SGSI necesitan basarse en los riesgos. La aplicación de un proceso de gestión del riesgo de seguridad de la información puede satisfacer este requisito. Existen muchos enfoques mediante los cuales se pueden determinar controles para implementar las opciones de tratamiento de riesgo elegidas.

La organización debería establecer, implementar y mantener un procedimiento para identificar los requisitos aplicables a:

- la selección de criterios para la evaluación del riesgo (7.2.2), el impacto del riesgo (7.2.3) y la aceptación del riesgo (7.2.4);
- la definición del alcance y los límites de la gestión del riesgo de seguridad de la información (7.3 y A.2);
- evaluación del riesgo (8.4);
- tratamiento del riesgo de (9.1) y la implementación de planes de reducción del riesgo (9.2 y Anexo F);
- el seguimiento, la revisión y la mejora de la gestión del riesgo (12.2);
- identificación de activos (B.1.3) y valoración de activos (B.2.3); y
- estimación del riesgo (véase ejemplos en E.2.1).

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

7 Establecimiento del contexto

7.1 Consideraciones generales

Entrada: Toda la información sobre la organización relevante al establecimiento del contexto para la gestión del riesgo de seguridad de la información.

Acción: Se debería establecer el contextos interno y externo para la gestión del riesgo de la seguridad de la información, que implica establecer los criterios básicos necesarios para la gestión del riesgo de seguridad de la información (7.2), definir el alcance y los límites (7.3), y establecer una organización apropiada que opere la gestión del riesgo de seguridad de la información (7.4).

Guía de implementación:

Es esencial determinar el propósito de la gestión del riesgo de seguridad de la información pues éste afecta el proceso global y en particular el establecimiento del contexto.

Este propósito puede ser:

- soporte de un SGSI;
- cumplimiento legal y evidencia de la debida diligencia;
- preparación de un plan de continuidad del negocio;
- preparación de un plan de respuesta a incidentes; y
- la descripción de los requisitos de seguridad de la información para un producto, un servicio o un mecanismo.

Orientación sobre implementación de los elementos del establecimiento del contexto necesarios para apoyar un SGSI se discute en.7.2, 7.3 y 7.4, a continuación.

Salida: La especificación de criterios básicos, el alcance y los límites, y la organización para el proceso de gestión del riesgo de seguridad de la información.

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

7.2 Criterios básicos

7.2.1 Enfoque de la gestión de riesgo

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diversos enfoques. El enfoque puede también ser diferente para cada iteración.

Se debería seleccionar o desarrollar un enfoque apropiado de gestión del riesgo que dirija los criterios básicos tales como: criterio de valoración de riesgos, criterio de evaluación del impacto, criterio de aceptación del riesgo.

De manera adicional, se debería que la organización evaluar si los recursos necesarios están disponibles para:

- realizar la evaluación del riesgo y establecer un plan de tratamiento de riesgos;
- definir e implementar políticas y procedimientos, incluyendo la implementación de los controles seleccionados;
- hacer el seguimiento (monitoring) de controles; y
- hacer el seguimiento (monitoring) del proceso de gestión del riesgo de seguridad de la información.

7.2.2 Criterio de valoración del riesgo

Se debería desarrollar criterios de valoración del riesgo para evaluar el riesgo de seguridad de la información de la organización considerando lo siguiente:

- el valor estratégico del proceso de la información del negocio;
- la criticidad de los activos de información implicados;

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- la importancia operacional y del negocio de la disponibilidad, de la confidencialidad y de la integridad; y

- las expectativas y percepciones de las partes interesadas, y las consecuencias negativas para la buena voluntad y reputación.

De manera adicional, el criterio de valoración del riesgo se puede utilizar para especificar las prioridades en el tratamiento de riesgos.

7.2.3 Criterios de impacto

NOTA: ISO 31000 utiliza un concepto de "criterios de consecuencia" en lugar de "criterios de impacto".

Los criterios de impacto deberían ser desarrollados y especificados en términos del grado de daño o costos para la organización causados por un evento de seguridad de la información considerando lo siguiente:

- nivel de clasificación del activo de la información afectado;

- brechas de la seguridad de la información (por ejemplo, pérdida de confidencialidad, de integridad y de disponibilidad);

- operaciones deterioradas (internas o con terceras partes);

- pérdida de negocios y de valor financiero;

- alteración de planes y de plazos; y

- daños a la reputación.

7.2.4 Criterios de aceptación del riesgo

Se debería desarrollar y especificar criterios de aceptación del riesgo. Los criterios de aceptación del riesgo dependen a menudo de las políticas de la organización, de las metas, de los objetivos y de los intereses de las partes interesadas (stakeholders).

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo se debería considerar lo siguiente:

- los criterios de aceptación del riesgo pueden incluir múltiples umbrales, con un nivel objetivo de riesgo deseado, pero con la previsión para que la alta dirección pueda aceptar riesgos sobre este nivel, bajo circunstancias definidas;
- el criterio de aceptación del riesgo puede ser expresado como el ratio del beneficio estimado (o de otro beneficio del negocio) sobre el riesgo estimado;
- diferentes criterios de aceptación del riesgo pueden aplicarse a diferentes clases de riesgo; y
- criterios de aceptación del riesgo pueden incluir requisitos para un tratamiento adicional futuro, por ejemplo, un riesgo puede ser aceptado si hay aprobación y compromiso para tomar la acción para reducirlo a un nivel aceptable dentro de un período de tiempo definido.

Los criterios de aceptación del riesgo pueden variar según cuánto tiempo se espera que exista el riesgo, por ejemplo, el riesgo se puede asociar a una actividad temporal o a corto plazo. Se debería fijar los criterios de aceptación del riesgo considerando lo siguiente:

- criterios del negocio;
- operaciones;
- tecnología;
- finanzas; y
- factores sociales y humanitarios.

Más información se puede encontrar en el Anexo A .

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

7.3 El alcance y los límites

La organización debería definir el alcance y los límites de la gestión del riesgo de seguridad de la información.

Es necesario definir el alcance del proceso de gestión del riesgo de seguridad de la información, para asegurar que todos los activos relevantes son tomados en cuenta en la evaluación de riesgos. Adicionalmente, es necesario identificar los límites para tratar esos riesgos que pudieran presentarse con estos límites.

Se debería recolectar información sobre la organización para determinar el entorno en el que opera y su importancia para el proceso de gestión del riesgo de seguridad de la información.

Cuando se define el alcance y los límites, la organización debería considere la siguiente información:

- los objetivos estratégicos del negocio, las estrategias y las políticas de la organización;
- los procesos del negocio;
- las funciones y estructura de la organización;
- la política de seguridad de la información de la organización;
- el enfoque global de la organización a la gestión del riesgo;
- los activos de información;
- las ubicaciones físicas de la organización y sus características geográficas;
- las restricciones que afectan la organización;
- las expectativas de las partes interesadas (stakeholders);
- el entorno socio-cultural; y
- la interfaz (es decir intercambio de información con el entorno).

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

De manera adicional, la organización debería proporcionar justificación para cualquier exclusión en el alcance.

Ejemplos de alcance de la gestión del riesgo pueden ser una aplicación de TI, infraestructura de TI, un proceso del negocio, o una parte definida de una organización.

Información adicional puede encontrarse en el Anexo A .

7.4 Organización para la gestión del riesgo de seguridad de la información

La organización y las responsabilidades para el proceso de gestión del riesgo de seguridad de la información deberían ser fijadas y mantenidas. Los siguientes son los roles y las responsabilidades principales de esta organización:

- desarrollo del proceso de gestión del riesgo de seguridad de la información conveniente para la organización;
- identificación y análisis de las partes interesadas;
- definición de roles y responsabilidades de todas las partes, tanto internas como externas a la organización;
- establecimiento de las relaciones requeridas entre la organización y las partes interesadas (stakeholders), así como la interfaz con las funciones de gestión del riesgo de alto nivel de la organización (por ejemplo, gestión del riesgo operacional), así como la interfaz con otros proyectos o actividades relevantes;
- definición de las rutas de escalamiento de decisiones; y
- especificación de los registros que se guardarán.

Esta organización debería sea aprobada por los directores apropiados de la organización.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

8 Evaluación del riesgo de seguridad de la información

8.1 Descripción general de la evaluación del riesgo de seguridad de la información

Entrada: Los criterios básicos, el alcance y los límites, y la organización para el proceso de gestión del riesgo de seguridad de la información que está siendo establecido.

Acción: Los riesgos deberían ser identificados, cuantificados o descritos cualitativamente, y priorizados contra criterios de valoración del riesgo y objetivos relevantes para la organización.

Guía de implementación:

Un riesgo es una combinación de las consecuencias que pueden seguir a la ocurrencia de un evento no deseado y de la probabilidad de la ocurrencia del evento. La evaluación del riesgo cuantifica o describe cualitativamente el riesgo y permite a los directores priorizar el riesgo de acuerdo con su percepción de la gravedad u otros criterios establecidos.

La evaluación del riesgo consiste en las siguientes actividades:

- identificación del riesgo (8.2);
- análisis del riesgo (8.3); y
- valoración del riesgo (8.4).

La evaluación del riesgo determina el valor de los activos de información, identifica las amenazas aplicables y las vulnerabilidades que existen (o podrían existir), identifica los controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y finalmente prioriza los riesgos derivados y los ordena contra el conjunto de criterios de valoración del riesgo en el contexto establecido.

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

La evaluación del riesgo es a menudo conducida en dos (o más) iteraciones. Primero se lleva cabo una evaluación de alto nivel para identificar riesgos potencialmente altos que requieran un análisis más profundo. La siguiente iteración puede implicar considerar una evaluación más a fondo del riesgo potenciales altos revelados en la iteración inicial. Cuando esto provea información insuficiente para evaluar el riesgo, entonces análisis adicionales detallados son efectuados, probablemente en parte del alcance total, y posiblemente utilizando un método diferente.

Le atañe a la organización seleccionar su propio enfoque a la evaluación del riesgo sobre la base de los objetivos y las metas de la evaluación de riesgos.

Discusiones sobre enfoques de la evaluación del riesgo de seguridad de la información pueden encontrarse en el Anexo E .

Salida: Una lista de los riesgos evaluados, priorizados de acuerdo al criterio de valoración de riesgos.

8.2 Identificación del riesgo

8.2.1 Introducción a la identificación del riesgo

El propósito de la identificación del riesgo es determinar qué podría suceder para causar una potencial perdida, y conocer mejor cómo, cuándo y por qué la pérdida podría suceder. Los pasos descritos en los sub capítulos siguientes deberían recolectar datos de entrada para la actividad de análisis del riesgo.

La identificación del riesgo debería incluir riesgos ya sea que su fuente se encuentre o no bajo control de la organización, aunque su fuente o causa no sea evidente.

NOTA: Las actividades descritas en los siguientes capítulos pueden ser realizadas en diferente orden dependiendo de la metodología aplicada.

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

8.2.2 Identificación de activos

Entrada: Alcance y límites de la evaluación del riesgo a ser realizada, lista de componentes con sus propietarios, ubicación, función, entre otros.

Acción: Los activos dentro del alcance establecido deberían ser identificados

Guía de implementación:

Un activo es cualquier cosa que tiene valor para la organización y que por lo tanto requiere protección. Para la identificación de los activos se debería tener en cuenta que un sistema de información es más que hardware y software.

La identificación de activos se debería realizar con un nivel adecuado de detalle tal que provea información suficiente para la evaluación del riesgo. El nivel de detalle utilizado en la identificación del activo va a influir en la cantidad de información general recolectada durante la evaluación del riesgo. El nivel puede ser refinado en más iteraciones de la evaluación del riesgo.

Se debería identificar al propietario de cada activo, con el fin de determinar quién es el responsable y quién debe rendir cuentas sobre el mismo. El propietario del activo puede no tener derecho de propiedad sobre el mismo, pero tiene responsabilidad por su producción, desarrollo, mantenimiento, uso y seguridad según corresponda. El propietario del activo es a menudo la persona más adecuada para determinar el valor del activo para la organización (véase 8.3.2 para evaluación de activo).

Los límites de la revisión son el perímetro de los activos de la organización definidos para ser gestionados por el proceso de gestión del riesgo de seguridad de la información.

Información adicional sobre la identificación y evaluación de activos relacionada con la seguridad de la información puede encontrarse en el Anexo B .

Salida: Una lista de activos a los cuales se les aplicará la gestión de riesgos, y una lista de los procesos de negocio relacionados a los activos y su relevancia.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

8.2.3 Identificación de las amenazas

Entrada: Información sobre amenazas obtenidas de la revisión de incidentes, propietarios de activos, usuarios y otras fuentes, incluyendo catálogos de amenazas externas.

Acción: Se deberían identificar las amenazas y sus fuentes.

Guía de implementación:

Una amenaza tiene el potencial de dañar los activos, tales como información, procesos y sistemas y por lo tanto a las organizaciones. Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas. Se deberían identificar las fuentes de amenazas, tanto accidentales como deliberadas. Una amenaza puede surgir desde dentro o fuera de la organización. Las amenazas deberían identificarse genéricamente y por tipo (por ejemplo, acciones no autorizadas, daños físicos, fallos técnicos) y cuando corresponda, identificar las amenazas particulares dentro de la clase general. Esto significa que no se pasaran por alto amenazas, incluyendo las inesperadas, pero el volumen de trabajo requerido es limitado.

Algunas amenazas pueden afectar a más de un activo. En estos casos ellas pueden causar diferentes impactos dependiendo qué activos sean afectados.

Se pueden obtener elementos de entrada a la identificación y estimación de la probabilidad de ocurrencia de amenazas (véase 8.3.3) de los propietarios o usuarios de activos, del personal de recursos humanos, de especialistas de gestión de las instalaciones físicas y de seguridad de la información, expertos en seguridad física, el departamento legal y otras organizaciones incluyendo cuerpos de la ley, autoridades meteorológicas, compañías de seguros y autoridades gubernamentales. También deberían considerarse aspectos culturales y del entorno cuando se tratan las amenazas.

En una evaluación en curso se debería considerar la experiencia interna de incidentes y amenazas pasadas. Donde sea relevante, puede valer la pena consultar otros catálogos de amenazas (tal vez específicos a una organización o negocio) para completar la lista de amenazas genéricas. Están disponibles catálogos y estadísticas de amenazas de grupos de la industria, gobiernos nacionales, grupos legales, compañías de seguro, entre otros.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Cuando utilizamos catálogos de amenazas, o los resultados de las primera evaluación de amenazas, se debería ser consciente del cambio continuo de las amenazas relevantes, especialmente si el entorno del negocio o los sistemas de información cambian.

Información adicional sobre los tipos de amenazas puede encontrase en el Anexo C .

Salida: Una lista de amenazas con la identificación del tipo de amenaza y sus fuentes.

8.2.4 Identificación de controles existentes

Entrada: Documentación de los controles, los planes de implementación de tratamiento de riesgos.

Acción: Se debería identificar los controles existentes y planificados.

Guía de implementación:

Se debería realizar una identificación de los controles existentes a fin de evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de controles. En suma, mientras se identifican los controles existentes se debería hacer un chequeo para asegurar que los controles están trabajando correctamente –una referencia a los informes de auditoría del SGSI ya existentes debería limitar el tiempo invertido en esta tarea–. Si un control no trabaja como se espera, podría causar vulnerabilidades. Se debería tomar en consideración la situación donde un control (o estrategia) seleccionado falla en operación y por lo tanto se requieren controles complementarios para enfrentar efectivamente al riesgo identificado.

Los controles que están planificados para ser implementados de acuerdo con los planes de implementación del tratamiento del riesgo deberían ser considerados de la misma manera que los que ya se han implementado.

Un control existente o planificado puede ser identificado como inefectivo, insuficiente, o no justificado. Si no es justificado o no es suficiente, se debería corroborar el control para determinar si debería ser eliminado, remplazado por otro control más adecuado, o si debería permanecer en su sitio (stay in place), por ejemplo, por razones de costo.

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Las siguientes actividades pueden ayudar a la identificación de controles existentes o planificados:

- revisar documentos conteniendo información sobre los controles (por ejemplo, planes para la implementación del tratamiento de riesgos). Si los procesos de gestión de seguridad de la información están bien documentados, todos los controles existentes o planificados y el estado de su implementación deberían estar disponibles;

- verificar con las personas responsables de la seguridad de la información (por ejemplo, oficial de seguridad de la información y oficial de sistemas de seguridad de la información, gerente de oficinas o administrador de operaciones) y con los usuarios en cuanto a que controles están realmente implementados para los procesos de información o sistemas en consideración;

- realizar una revisión en el sitio (on-site) de los controles físicos, comparando aquello implementado con la lista de los controles que deberían estar allí, y chequeando aquello implementado en cuanto a si esta trabajado correcta y efectivamente, o

- revisar los resultados de auditorías.

Salida: Una lista de todos los controles existentes y planificados, su estado de implementación y de uso.

8.2.5 Identificación de vulnerabilidades

Entrada: Una lista de amenazas conocidas, listas de activos y controles existentes.

Acción: Se debería identificar las vulnerabilidades que pueden ser explotadas por amenazas para causar daños a los activos o a la organización.

Guía de implementación:

Se podrían identificar vulnerabilidades en las siguientes áreas:

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- organización;
- procesos y procedimientos;
- rutinas de gestión;
- personal;
- entorno físico;
- configuración de sistemas de información;
- hardware, software o equipos de comunicación; y
- dependencias de partes externas.

La presencia de una vulnerabilidad no causa daño en sí misma, ya que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una correspondiente amenaza puede no requerir de la implementación de un control, pero debería ser reconocida y establecer un seguimiento (monitoring) en caso de cambios. Debería señalarse que un control implementado incorrectamente o funcionando mal o un control siendo utilizado incorrectamente puede él mismo, ser una vulnerabilidad. Un control puede ser efectivo o inefectivo dependiendo del entorno en que opera. Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar en un riesgo.

Las vulnerabilidades pueden estar relacionadas a propiedades de los activos que pueden ser utilizadas en un sentido, o para un propósito, distinto a la intención con la cual el activo fue comprado o hecho. Necesitan considerarse vulnerabilidades derivadas de diferentes fuentes, por ejemplo, aquellas intrínsecas o extrínsecas a los activos.

Ejemplos de vulnerabilidades y métodos para la evaluación de vulnerabilidades pueden encontrase en el Anexo D .

Salida: Una lista de las vulnerabilidades en relación a los activos, amenazas y controles; una lista de las vulnerabilidades que no se relacionaron con ninguna amenaza identificada para revisión.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

8.2.6 Identificación de consecuencias

Entrada: Una lista de activos, una lista de procesos de negocios, y una lista de amenazas y vulnerabilidades, cuando sea apropiado, relacionada a los activos y su relevancia.

Acción: Se debería identificar las consecuencias que las pérdidas de confidencialidad, integridad y disponibilidad puedan tener en los activos.

Guía de implementación:

Una consecuencia puede ser: pérdida de eficacia, condiciones adversas de funcionamiento, pérdida del negocio, reputación, daño, entre otros.

Esta actividad identifica los daños o consecuencias para la organización que podrían causarse en el escenario de un incidente. El escenario de un incidente es la descripción de una amenaza explotando una cierta vulnerabilidad o un conjunto de vulnerabilidades en un incidente de seguridad de la información. El impacto del escenario del incidente va a ser determinado considerando el criterio de evaluación del impacto definido durante la actividad de establecimiento del contexto. Este puede afectar uno o más activos o parte de un activo. Por lo tanto, los activos pueden tener asignados valores tanto por su costo financiero como debido a las consecuencias al negocio si ellos son dañados o comprometidos. Las consecuencias pueden ser de naturaleza temporal o pueden ser permanentes como en el caso de la destrucción de un activo.

Las organizaciones deberían identificar las consecuencias operacionales de escenarios de incidentes en términos de (pero no limitados a):

- tiempo de investigación y de reparación;
- (trabajo) tiempo perdido;
- perdida de oportunidad;
- salud y seguridad;
- costos financieros de habilidades específicas para reparar los daños; y

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- imagen, reputación y credibilidad.

Detalles sobre la evaluación de vulnerabilidades técnicas pueden encontrase en B.3.

Salida: Una lista de escenarios de incidentes con sus consecuencias relacionadas a activos y procesos de negocio.

8.3 Análisis del riesgo

8.3.1 Metodologías de análisis del riesgo

El análisis del riesgo puede llevarse a cabo con diversos grados de detalle en función de la criticidad de los activos, el alcance de las vulnerabilidades conocidas, y los incidentes anteriores en los que se vio involucrada la organización. Una metodología de análisis puede ser cualitativa o cuantitativa, o una combinación de estas, dependiendo de las circunstancias. En la práctica, un análisis cualitativo es utilizado a menudo primero para obtener una indicación general del nivel del riesgo y para revelar los riesgos mayores. Luego puede ser necesario llevar a cabo un análisis más específico o cuantitativo sobre los riesgos mayores porque es usualmente menos complejo y menos costoso llevar a cabo análisis cualitativos que cuantitativos.

La forma del análisis debería ser consistente con los criterios de valoración del riesgo desarrollados como parte del establecimiento del contexto.

Más detalles de la metodología de estimación son descriptos a continuación:

a) Análisis cualitativo del riesgo:

El análisis cualitativo del riesgo utiliza una escala de clasificación de atributos para describir la magnitud de consecuencias potenciales (por ejemplo, Baja, Media, Alta) y la probabilidad de que esa consecuencia pueda ocurrir. Una ventaja del análisis cualitativo es su facilidad de comprensión por todo el personal relevante, mientras que una desventaja es la dependencia de la elección subjetiva de la escala.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Estas escalas pueden ser adaptadas o ajustadas para adaptarse a las circunstancias y descripciones diferentes pueden ser utilizadas para riesgos diferentes. Puede utilizarse el análisis cualitativo:

- como una actividad de selección inicial para identificar los riesgos que requieren análisis más detallado;
- cuando este tipo de análisis es apropiado para las decisiones; y
- cuando los datos numéricos o los recursos son inadecuados para un análisis cualitativo.

Cuando esté disponible, el análisis cualitativo debería utilizar información basada en datos y hechos reales.

b) Análisis cuantitativo de riesgos:

El análisis cuantitativo del riesgo utiliza una escala con valores numéricos (en lugar de las escalas descriptivas utilizadas en el análisis cualitativo) tanto para consecuencia como para probabilidad, utilizando datos de una variedad de fuentes. La calidad del análisis depende de la exactitud y de la completitud de los valores numéricos y de la validez de los modelos utilizados. El análisis cuantitativo del riesgo utiliza en muchos casos datos históricos de incidentes proporcionando la ventaja de que estos pueden estar directamente relacionados con los objetivos de seguridad de la información y preocupaciones de la organización. Una desventaja es la falta de datos sobre nuevos riesgos o debilidades de seguridad de la información. Una desventaja del enfoque cuantitativo puede darse cuando no están disponibles los datos auditables, de hechos, creando entonces una ilusión del valor y exactitud de la evaluación de riesgos.

El modo en que son expresadas las consecuencias y las probabilidades, y el modo en que son combinadas para proporcionar el nivel de riesgos, pueden variar de acuerdo al tipo de riesgo y el propósito con que va a ser utilizada la salida de la evaluación de riesgos. se debería que la incertidumbre y variabilidad tanto de las consecuencias como de la probabilidad sean consideradas en el análisis y comunicadas efectivamente.

8.3.2 Evaluación de consecuencias

Entrada: Una lista de escenarios de incidentes relevantes identificados, incluyendo identificación de amenazas, vulnerabilidades, activos afectados, consecuencias sobre los activos y procesos del negocio.

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Acción: Se debería evaluar el impacto sobre el negocio de la organización que pudiera resultar de incidentes posibles o reales de la seguridad de la información, teniendo en cuenta las consecuencias de una violación de la seguridad de la información, tales como pérdida de confidencialidad, integridad o disponibilidad de los activos.

Guía de implementación: Después de la identificación de todos los activos bajo revisión, se debería tener en cuenta los valores asignados a dichos activos cuando se evalúan las consecuencias.

Un concepto de impacto en el negocio es utilizado para medir las consecuencias. El valor del impacto en el negocio puede ser expresado en forma cualitativa y cuantitativa, pero cualquier método de asignación de valores monetarios generalmente puede proporcionar más información para la toma de decisiones y por lo tanto facilitar un proceso de toma de decisiones más eficiente.

La valoración de activos comienza con la clasificación de activos de acuerdo a su criticidad, en términos de la importancia de los activos en el cumplimiento de los objetivos del negocio de la organización. La valoración es determinada entonces utilizando dos medidas:

- el valor de reposición del activo: el costo de la recuperación limpia y la sustitución de la información (si es del todo posible); y

- las consecuencias en el negocio por la pérdida así como las o compromiso del activo, potenciales consecuencias adversas al negocio y/o consecuencias legales o reglamentarias por la divulgación, modificación, indisponibilidad y/o destrucción de información, y otros activos de información.

Esta valoración se puede determinar a partir de un análisis de impacto en el negocio. El valor determinado por las consecuencias para el negocio, es usualmente significativamente mayor que el costo de una simple sustitución, dependiendo de la importancia del activo para la organización en el cumplimiento de los objetivos de negocio.

La valoración de activos es un factor clave en la evaluación del impacto de un escenario de incidente, porque el incidente puede afectar más de un activo (por ejemplo, activos dependientes), o solo una parte de un activo. Diferentes amenazas y vulnerabilidades tendrán diferentes impactos en los activos, tales como una pérdida de confidencialidad,

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

integridad o disponibilidad. La evaluación de las consecuencias está relacionada entonces con la evaluación de los activos basada en el análisis del impacto sobre el negocio.

Las consecuencias o impactos en el negocio pueden ser determinadas por los resultados de modelos de un evento o conjunto de eventos, o por la extrapolación de estudios experimentales o datos del pasado.

Las consecuencias pueden ser expresadas en términos monetarios, técnicos o criterios de impacto humano, u otros criterios relevantes para la organización. En algunos casos, es requerido más de un valor numérico para especificar las consecuencias para distintos momentos, lugares, grupos o situaciones.

Las consecuencias en el tiempo y las finanzas deberían ser medidas con el mismo enfoque utilizado en la probabilidad de amenazas y vulnerabilidades. La consistencia tiene que ser mantenida en el enfoque cuantitativo y cualitativo.

Más información sobre la evaluación de activos y la evaluación del impacto puede encontrase en el Anexo B .

Salida: Una lista de las consecuencias evaluadas en un escenario de incidente expresadas con respecto a los activos y criterios de impacto.

8.3.3 Evaluación de probabilidad de incidentes

Entrada: Una lista de los escenarios de incidentes relevantes identificados, incluyendo identificación de amenazas, activos afectados, vulnerabilidades explotadas y consecuencias para los activos y procesos del negocio. Además, listas de todos los controles existentes y planificados, su efectividad, y estado de implementación y uso.

Acción: Se debería evaluar la probabilidad (de ocurrencia) de escenarios de incidentes.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Guía de implementación:

Después de identificar los escenarios de incidentes, es necesario evaluar la probabilidad de ocurrencia de cada escenario y el impacto que produzca, utilizando técnicas de análisis cualitativo o cuantitativo. Se debería tomar en cuenta cuan a menudo ocurre la amenaza y cuan fácilmente las vulnerabilidades pueden ser explotadas, considerando:

- experiencia y estadísticas aplicables para probabilidad de amenazas;
- para fuentes deliberadas de amenaza: la motivación y capacidades, que cambian con el tiempo, y los recursos disponibles a posibles atacantes, así como la percepción del atractivo y la vulnerabilidad de los activos para un posible atacante;
- para fuentes accidentales de amenazas: factores geográficos, por ejemplo, proximidad de plantas químicas o petroleras, la posibilidad de condiciones extremas del clima, y factores que podrían influir en errores humanos y mal funcionamiento de equipamiento;
- las vulnerabilidades, tanto individualmente como sumadas; y
- controles existentes y cuan efectivamente estos reducen las vulnerabilidades.

Por ejemplo, un sistema de información puede tener una vulnerabilidad para las amenazas de enmascaramiento (masquerading) de identidad de usuario y el uso indebido de recursos. La vulnerabilidad de enmascaramiento (masquerading) de la identidad de un usuario puede ser alta debido a la falta de autenticación de usuario. Por otro lado, la probabilidad del uso indebido del recurso puede ser baja, a pesar de la falta de autenticación de usuario, porque las formas de uso indebido de recursos están limitadas.

Dependiendo de la necesidad de exactitud, los activos podrían ser agrupados, o podría ser necesario dividir los activos en sus elementos y referir los escenarios a los elementos. Por ejemplo, a través de ubicaciones geográficas, la naturaleza de las amenazas para el mismo tipo de activos puede cambiar, o la efectividad de los controles existentes puede variar.

Salida: La probabilidad de escenarios de incidentes (cuantitativa o cualitativa)

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

8.3.4 Determinación del nivel de riesgo

Entrada: Una lista de escenarios de incidentes con sus consecuencias relacionadas con los activos y procesos de negocio y su probabilidad (cuantitativa o cualitativa).

Acción: Se debería determinar el nivel del riesgo para todos los escenarios de incidentes relevantes

Guía de implementación:

El análisis del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. Esos valores pueden ser cuantitativos o cualitativos. El análisis del riesgo está basado en las consecuencias y probabilidades evaluadas. Adicionalmente, este puede considerar costo beneficio, las preocupaciones de las partes interesadas (stakeholders), y otras variables, que sean apropiadas para la valoración del riesgo. El riesgo estimado es una combinación de la probabilidad de un escenario de incidente y sus consecuencias.

Ejemplos de diferentes métodos o enfoques de análisis del riesgo de seguridad de la información pueden encontrase en el Anexo E .

Salida: Una lista de riesgos con valores asignados a niveles.

8.4 Valoración del riesgo

Entrada: Una lista del riesgo con valores asignados a niveles y criterios de valoración de riesgos.

Acción: Se debería comparar los niveles del riesgo contra los criterios de valoración del riesgo y los criterios de aceptación de riesgos.

Guía de implementación:

La naturaleza de las decisiones relativas a la valoración del riesgo y a los criterios de valoración de riesgos, que van a ser utilizados para tomar estas decisiones, se deberían de

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

haber definido al establecer el contexto. Estas decisiones y el contexto deberían ser revisados con más detalle en esta etapa cuando se conoce más sobre los riesgos particulares identificados. Para evaluar los riesgos, las organizaciones deberían comparar los riesgos estimados (utilizando métodos seleccionados o enfoques como los discutidos en el Anexo E) con los criterios de valoración del riesgo definidos durante el establecimiento del contexto.

Los criterios de valoración del riesgo utilizados para tomar decisiones deberían ser consistentes con el contexto interno y externo de gestión del riesgo de seguridad de la información y tomar en cuenta los objetivos de la organización y las visiones de las partes interesadas (stakeholders) entre otros. Las decisiones tomadas en la actividad de valoración del riesgo están basadas principalmente en el nivel de riesgo aceptable. De todos modos, se debería también considerar las consecuencias, probabilidades y grado de confianza en el análisis e identificación de riesgos. La suma de múltiples riesgos bajos o medios puede resultar en riesgos totales mucho más altos, y necesitan ser manejados de manera acorde.

Las consideraciones deberían incluir:

- propiedades de seguridad de la información: si un criterio no es relevante para la organización (por ejemplo, pérdida de confidencialidad), entonces pueden no ser relevantes todos los riesgos sobre los que tiene efecto este criterio;

- la importancia del proceso de negocio o actividad soportada por un activo particular o por un conjunto de activos: si se determina que el proceso es de baja importancia, a los riesgos asociados con este se debería darle una consideración más baja que a aquellos riesgos que impactan en procesos o actividades más importantes;

La valoración del riesgo utiliza el conocimiento del riesgo obtenido en el análisis de riesgo para tomar decisiones sobre acciones futuras. Las decisiones deberían incluir:

- cuando una actividad debería ser emprendida; y

- prioridades para el tratamiento del riesgo considerando niveles estimados de los riesgos.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Salida: Una lista de riesgos priorizados de acuerdo a los criterios de valoración del riesgo en relación a los escenarios de incidentes que conducen a estos riesgos.

9 Tratamiento del riesgo de seguridad de la información

9.1 Descripción general del tratamiento del riesgo

Entrada: Una lista del riesgo priorizada de acuerdo a los criterios de valoración del riesgo en relación a los posibles escenarios que llevan a tales riesgos.

Acción: Se debería seleccionar controles para reducir, retener, evitar, o transferir los riesgos y definir un plan de tratamiento de riesgos.

Guía de Implementación:

Hay cuatro opciones disponibles para el tratamiento de riesgo: modificación del riesgo (véase 9.2), retención del riesgo (véase 9.3), evitar el riesgo (véase 9.4) y compartir el riesgo (véase 9.5).

La Figura 3 ilustra las actividades del tratamiento del riesgo dentro de los procesos de gestión del riesgo de seguridad de la información tal como fueron presentados en la Figura 2 .

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

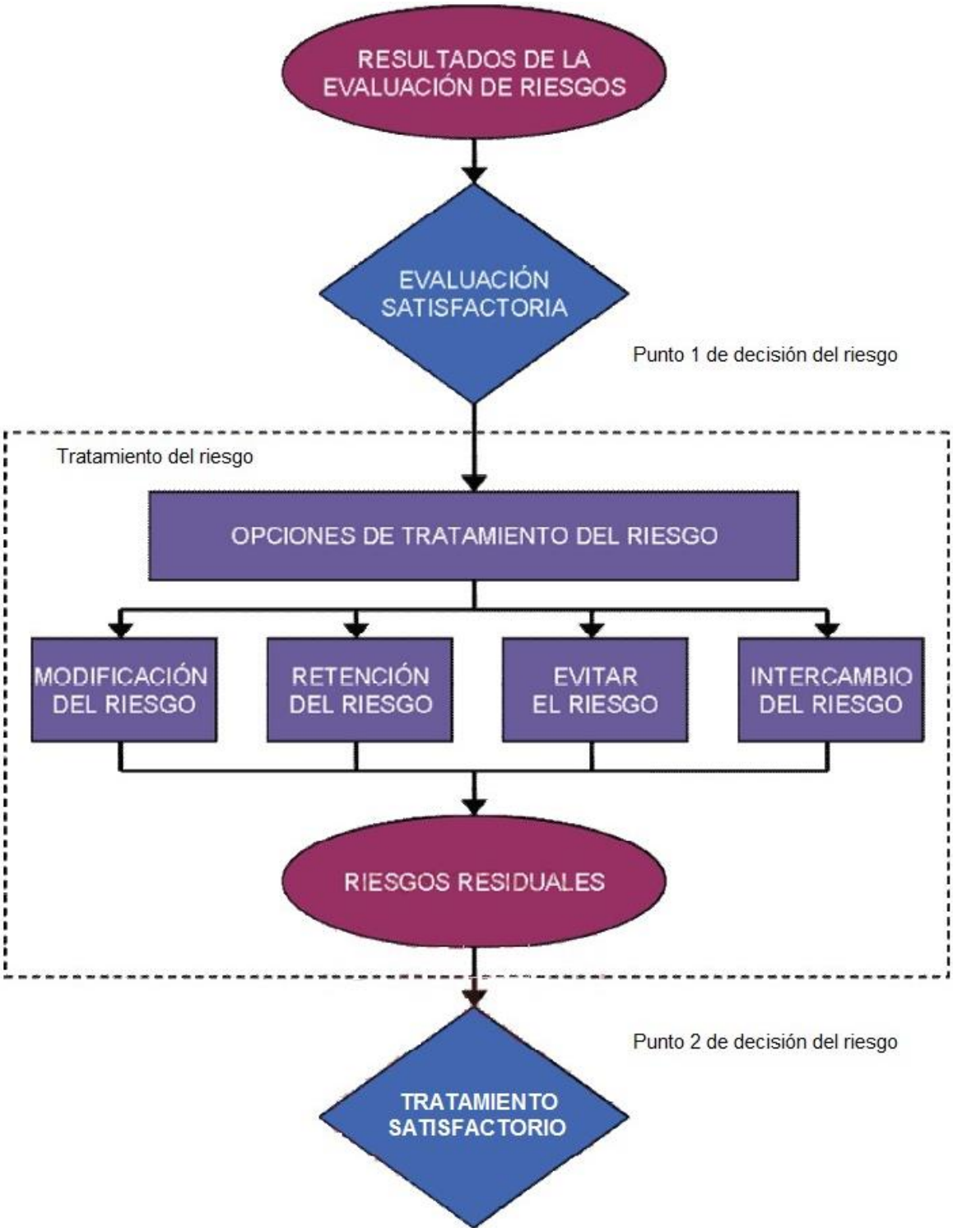

Figura 3 – La actividad tratamiento del riesgo

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Las opciones de tratamiento del riesgo deberían ser seleccionadas basándose en el resultado de la evaluación de riesgos, el costo esperado de implementar dichas opciones y los beneficios esperados de las mismas.

Cuando se pueden obtener grandes reducciones en los riesgos con gastos relativamente bajos, tales opciones deberían ser implementadas. Opciones adicionales de mejora podrían no ser económicas y se necesitaría aplicar un juicio para evaluar si son justificables.

En general, las consecuencias adversas de los riesgos deberían ser minimizadas tanto como sea razonablemente practicable e independientemente de cualquier criterio absoluto. La alta dirección debería considerar riesgos raros pero severos. En tales casos, puede ser necesario implementar controles que no son justificables en el terreno estrictamente económico (por ejemplo, controles de continuidad del negocio que cubran riesgos altos específicos).

Las cuatro opciones para el tratamiento del riesgo no son mutuamente excluyentes. Algunas veces una organización puede beneficiarse substancialmente utilizando una combinación de opciones tales como reducir la probabilidad de los riesgos, reduciendo sus consecuencias, e intercambiando o reteniendo cualquier riesgo residual.

Algunos tratamientos del riesgo pueden efectivamente apuntar a más de un riesgo (por ejemplo, concientización y entrenamiento en la seguridad de la información). Se debería definir un plan de tratamiento de riesgos, que identifique claramente el orden de prioridad y los plazos de implementación de los tratamientos individuales de riesgos. Las prioridades pueden ser establecidas utilizando varias técnicas, incluyendo un ranking de riesgos y análisis costo-beneficio. Es la responsabilidad de la alta dirección de la organización decidir el balance entre los costos de implementar los controles y la asignación de presupuesto.

La identificación de los controles existentes puede determinar que los mismos exceden las necesidades actuales, en términos de comparación de costos, incluyendo mantenimiento. Si se considera eliminar controles redundantes o innecesarios (especialmente si los controles tienen altos costos de mantenimiento) se debería tomar en cuenta factores de costos y de la seguridad de la información. Ya que los controles pueden influir unos en otros, eliminar controles redundantes puede reducir el nivel de la seguridad implementada. Adicionalmente, puede ser más barato dejar los controles redundantes o innecesarios en lugar de quitarlos.

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Se debería considerar opciones en el tratamiento del riesgo tomando en cuenta:

- cómo el riesgo es percibido por las partes afectadas; y
- las maneras más apropiadas de comunicarse con esas partes.

El riesgo para la organización es la falta de cumplimiento por lo que se debería implementar opciones de tratamiento para limitar esta posibilidad. Todas las limitaciones - organizacionales, técnicas, estructurales, entre otros. - que sean identificadas durante la actividad de establecimiento del contexto deberían ser tomadas en cuenta durante el tratamiento de riesgos.

Una vez que el plan de tratamiento del riesgo ha sido definido, se necesita determinar los riesgos residuales. Esto involucra una actualización o re-iteración de la evaluación de riesgos, tomando en cuenta los efectos esperados del tratamiento del riesgo propuesto. Si el riesgo residual aún no satisface el criterio de aceptación de la organización, puede ser necesaria otra iteración de tratamiento del riesgo antes de proceder a la aceptación de riesgos.

Salida: Plan de tratamiento del riesgo y riesgos residuales sujetos a la decisión de aceptación por la alta dirección de la organización.

9.2 Modificación del riesgo

Acción: El nivel del riesgo debería ser gestionado mediante la introducción, remoción o alteración de controles de forma tal que el riesgo residual pueda ser re-evaluado como aceptable.

Guía de implementación:

Se debería seleccionar controles apropiados y justificados que cumplan los requerimientos identificados por la evaluación del riesgo y el tratamiento de riesgos. Esta selección debería también tome en cuenta el costo y tiempos de implementación de controles, o aspectos técnicos, del ambiente y culturales. En general es posible bajar el costo de propiedad de un sistema con controles de seguridad de la información seleccionados apropiadamente.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

En general, los controles pueden proveer uno o más de los siguientes tipos de protección: corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, seguimiento (monitoring) y concientización. Durante la selección del control, es importante balancear el costo de adquisición, implementación, administración, operación, seguimiento (monitoring), y mantenimiento de los controles contra el valor de los activos que están siendo protegidos. Por otra parte, se debería considerar el retorno de la inversión en términos de la reducción del riesgo y el potencial para explotar nuevas oportunidades de negocio que se alcanzan a partir de ciertos controles. Adicionalmente, se debería considerar las habilidades especializadas que podrían ser necesarias para definir e implementar nuevos controles o modificar los existentes.

La norma ISO/IEC 27002 provee información detallada sobre controles.

Hay muchas restricciones que pueden afectar la selección de controles. Restricciones técnicas tales como requerimientos de desempeño, administración (requerimientos de soporte operacional) y problemas de compatibilidad pueden obstaculizar el uso de ciertos controles o pueden inducir al error humano resultando en una anulación del control, dando una falsa sensación de seguridad o incluso aumentando el riesgo más allá de no tener el control (por ejemplo,: requerir claves complejas sin entrenamiento adecuado puede llevar a los usuarios a escribir sus claves en papel). Es más, puede darse el caso que un control pueda afectar el desempeño. La alta dirección debería intentar identificar una solución que satisfaga los requerimientos de desempeño mientras que se garantiza una suficiente seguridad de la información. El resultado de este paso es una lista de posibles controles, con su costo, beneficio y prioridad de implementación.

Se debería tomar en cuenta varias restricciones cuando se seleccionen controles y durante su implementación.

En general se consideran las siguientes:

- restricciones de tiempo;
- restricciones financieras;
- restricciones técnicas;
- restricciones operacionales;

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- restricciones culturales;
- restricciones éticas;
- restricciones del entorno;
- facilidad de uso;
- restricciones de personal; y
- restricciones de la integración de controles nuevos y ya existentes.

Más información sobre las restricciones para la reducción del riesgo puede ser encontrada en el Anexo F .

9.3 Retención del riesgo

Acción: La decisión de retener el riesgo sin ninguna acción adicional debería ser tomada dependiendo de la valoración de los riesgos.

Guía de Implementación:

Si el nivel de riesgo satisface el criterio de aceptación de riesgos, no hay necesidad de implementar controles adicionales y el riesgo puede ser retenido.

9.4 Evitar el riesgo

Acción: Se debería evitar la actividad o condición que hace posible a un riesgo en particular.

Guía de implementación:

Cuando los riesgos identificados son considerados muy altos, o los costos de implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar la decisión de evitar el riesgo completamente, retirándose de una actividad planeada o existente o de un conjunto de actividades, o cambiando las condiciones sobre las cuales la actividad es

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

operada. Por ejemplo, para los riesgos causados por la naturaleza, puede ser más efectivo desde el punto de vista de costos la alternativa de mover las instalaciones de procesamiento a un lugar donde el riesgo no existe o esté bajo control.

9.5 Compartir el riesgo

Acción: El riesgo debería ser compartido con otra parte que pueda gestionar más eficazmente el riesgo particular en función de la valoración del riesgo.

Guía de implementación:

El riesgo compartido exige una decisión de compartir ciertos riesgos con las partes externas. Compartir un riesgo puede crear nuevos riesgos o modificar los riesgos existentes identificados. Por lo tanto, puede ser necesario el tratamiento adicional de riesgos.

Compartir puede hacerse por medio de un seguro que soportará las consecuencias, o por la subcontratación de un socio cuya función será la de supervisar el sistema de información y tomar acciones inmediatas para detener un ataque antes de que este alcance a un nivel definido de daño.

Cabe señalar que puede ser posible compartir la responsabilidad de gestionar el riesgo, pero normalmente no es posible compartir la responsabilidad por un impacto. Los clientes suelen atribuir un impacto adverso como si fuera una falla de la organización.

10 Aceptación del riesgo de seguridad de la información

Entrada: Plan de tratamiento del riesgo y evaluación del riesgo residual sujeto a la aceptación de la decisión de la dirección de la organización.

Acción: La decisión de aceptar los riesgos y responsabilidades para la decisión deberían ser hechas y registradas formalmente.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Guía de implementación:

Los planes de tratamiento del riesgo deberían describir cómo se evaluaron los riesgos y se van a tratar de cumplir los criterios de aceptación del riesgo (véase 7.2). Esto es importante para los directores responsables de revisar y aprobar las propuestas de planes de tratamiento del riesgo y riesgos residuales resultantes, y de registrar todas las condiciones asociadas con dicha aprobación.

Los criterios de aceptación del riesgo pueden ser más complejos que tan solo determinar si un riesgo residual cae por encima o por debajo de un umbral único.

En algunos casos el nivel de riesgo residual no podrá cumplir con criterios de aceptación de riesgo porque los criterios que se aplican no tienen en cuenta las circunstancias imperantes. Por ejemplo, se podría argumentar que es necesario aceptar los riesgos porque los beneficios que acompañan a los riesgos son muy atractivos, o porque el costo de la reducción del riesgo es demasiado alto. Tales circunstancias indican que los criterios de aceptación del riesgo son inadecuados y deberían si es posible ser objeto de revisión. Sin embargo, no siempre es posible revisar los criterios de aceptación de riesgo de manera oportuna. En tales casos, los tomadores de decisiones pueden tener que aceptar los riesgos que no cumplen con los criterios normales de aceptación. Si esto es necesario, los tomadores de decisión deberían explícitamente comentar acerca de los riesgos e incluir una justificación de la decisión de ignorar los criterios normales de aceptación de riesgos.

Salida: Una lista de los riesgos aceptados con la justificación de aquellos que no cumplen con los criterios normales de aceptación del riesgo de la organización.

11 Comunicación y consulta del riesgo de seguridad de la información

Entrada: Toda la información del riesgo obtenidos de las actividades de gestión del riesgo (véase Figura 2).

Acción: La información acerca de los riesgos debería ser intercambiada y/o compartida entre los tomadores de decisiones y otros interesados.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Guía de implementación:

La comunicación del riesgo es una actividad para lograr un acuerdo sobre la forma de gestionar riesgos intercambiando y/o compartiendo información sobre riesgo entre los tomadores de decisiones y otros interesados. La información incluye, pero no se limita a la existencia, la naturaleza, la forma, la probabilidad, la gravedad, el tratamiento y la capacidad de aceptación de los riesgos.

La comunicación eficaz entre los interesados es importante, ya que esto puede tener un impacto significativo sobre las decisiones que deben tomarse. La comunicación se asegurará que los responsables de la aplicación de gestión de riesgos, y aquellos con intereses creados comprendan la base sobre la cual se toman las decisiones y por qué son necesarias acciones particulares. La comunicación es bidireccional.

Las percepciones de riesgo pueden variar debido a las diferencias en los supuestos, los conceptos y las necesidades, asuntos y preocupaciones de las partes interesadas en lo que se refiere al riesgo o los asuntos objeto de discusión. Las partes interesadas probablemente emitan juicio sobre la capacidad de aceptación de riesgos. Esto es especialmente importante para garantizar que la percepción del riesgo de las partes interesadas, así como sus percepciones de los beneficios, puedan ser identificadas y documentadas, y las razones subyacentes claramente entendidas y abordadas.

La comunicación del riesgo debería llevarse a cabo con el fin de:

- ofrecer garantías de los resultados de la gestión del riesgo de la organización;
- recopilar información sobre los riesgos;
- compartir los resultados de la evaluación del riesgo y presentar el plan de tratamiento de riesgos;
- evitar o reducir la ocurrencia y la consecuencia de las violaciones de seguridad de la información debido a la falta de comprensión mutua entre los tomadores de decisiones y los interesados;
- apoyar la toma de decisiones;

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- obtener nuevos conocimientos en seguridad de la información;
- coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente;
- dar a los tomadores de decisión y los interesados un sentido de responsabilidad acerca de los riesgos;
- mejorar el conocimiento.

Una organización debería desarrollar planes de comunicación del riesgo para las operaciones normales, así como para situaciones de emergencia. Por lo tanto, la actividad de comunicación del riesgo debería ser llevada a cabo continuamente.

La coordinación entre los principales tomadores de decisiones y los interesados pueden lograrse mediante la formación de un comité donde puede tener lugar el debate acerca de los riesgos, sus prioridades, tratamiento apropiado, y su aceptación.

Es importante cooperar con las unidades apropiadas de relaciones públicas o comunicaciones dentro de la organización para coordinar todas las tareas relacionadas con la comunicación de riesgos. Esto es crucial en la eventualidad de acciones de comunicación de actividades de crisis, por ejemplo, en respuesta a incidentes particulares.

Salida: La comprensión continua del proceso de gestión del riesgo de seguridad de la información de la organización y sus resultados.

12 Seguimiento y revisión del riesgo de seguridad de la información

12.1 Seguimiento y revisión de los factores de riesgos

Entrada: Toda la información obtenida de las actividades de gestión del riesgo (véase Figura 2).

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Acción: Se debería hacer el seguimiento y revisión de los riesgos y sus factores (es decir, el valor de los activos, los impactos, las amenazas, vulnerabilidades, la probabilidad de ocurrencia) para identificar cualquier cambio en el contexto de la organización en una etapa temprana, y para mantener una visión completa de los riesgos.

Guía de implementación:

Los riesgos no son estáticos. Las amenazas, vulnerabilidades, probabilidades o consecuencias pueden cambiar bruscamente sin ningún tipo de indicación. Por lo tanto, el constante seguimiento es necesario para detectar estos cambios. Esto puede ser realizado apoyado por servicios externos que proporcionan información observando nuevas amenazas o vulnerabilidades.

Las organizaciones deberían asegurar que se haga el seguimiento continuo de lo siguiente:

- nuevos activos que se han incluido en el alcance de la gestión del riesgo;
- modificaciones necesarias del valor de los activos, por ejemplo, debido a los cambios en los requisitos del negocio;
- nuevas amenazas que podrían estar activas tanto fuera como dentro de la organización y que no hayan sido evaluadas;
- posibilidad de que vulnerabilidades nuevas o en aumento puedan permitir a las amenazas explotar estas vulnerabilidades nuevas o modificadas;
- vulnerabilidades identificadas para determinar aquellos expuestos destinados a convertirse en las nuevas o re-emergentes amenazas;
- aumento del impacto o consecuencias de las amenazas, vulnerabilidades y riesgos evaluados que sumados resultan en un nivel inaceptable de riesgo; y
- información sobre incidentes de seguridad.

Las nuevas amenazas, vulnerabilidades o cambios en la probabilidad o las consecuencias pueden aumentar los riesgos evaluados previamente como del nivel más bajo. La revisión de riesgos bajos y aceptados debería considerar cada riesgo en forma separada y también como un todo, a fin de evaluar su impacto potencial acumulado. Si los riesgos no se encuentran en o bajo la categoría de riesgo aceptable, deberían ser tratados utilizando una o varias de las opciones consideradas en el capítulo 9 .

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Los factores que afectan la probabilidad y consecuencias de las amenazas que ocurren podrían cambiar, al igual que los factores que afectan a la idoneidad o el coste de las distintas opciones de tratamiento. Los principales cambios que afectan a la organización deberían ser motivo para una revisión más específica. Por lo tanto, las actividades de seguimiento del riesgo deberían ser repetidas regularmente y las opciones seleccionadas para el tratamiento del riesgo sean revisadas periódicamente.

El resultado de las actividades de seguimiento del riesgo puede ser la entrada a otras actividades de revisión de riesgos. La organización debería revisar todos los riesgos periódicamente y cuando se produzcan cambios importantes.

Salida: La alineación continua de la gestión del riesgo con los objetivos del negocio de la organización y con los criterios de aceptación del riesgo.

12.2 Seguimiento, revisión y mejora de la gestión de riesgos

Entrada: Toda la información obtenida de las actividades de gestión del riesgo (véase Figura 2).

Acción: El proceso de gestión del riesgo de seguridad de la información deberían ser continuamente supervisado, revisado y mejorado, según sea necesario y apropiado.

Guía de implementación:

El seguimiento permanente y la revisión son necesarios para garantizar que el contexto, los resultados de la evaluación de los riesgos y tratamiento, así como los planes de gestión, siguen siendo relevantes y adecuados a las circunstancias.

La organización debería asegurarse que el proceso de gestión del riesgo de seguridad de la información y las actividades relacionadas, siguen siendo apropiados en las circunstancias actuales y son seguidos. Cualquier mejora al proceso o acciones necesarias para mejorar el cumplimiento con el proceso deberían ser notificada a los directores apropiados para tener la seguridad que:

- no existe ningún riesgo o elemento de riesgo pasado por alto o subestimado;

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

- las acciones necesarias son adoptadas; y
- las decisiones se toman para proporcionar una comprensión realista del riesgo y capacidad de respuesta.

Adicionalmente, que la organización debería verificar regularmente que los criterios utilizados para medir el riesgo y sus elementos siguen siendo válidos y coherentes con los objetivos del negocio, las estrategias y políticas, y que los cambios en el contexto del negocio se toman en cuenta adecuadamente durante el proceso de gestión del riesgo de seguridad de la información. Esta actividad de seguimiento y revisión debería abordar (pero no esté limitada a):

- contexto de competitividad;
- enfoque de evaluación de riesgos;
- valor y categorías de los activos;
- criterios de impacto;
- criterios de valoración de riesgos;
- criterios de aceptación de riesgos;
- coste total de propiedad; y
- recursos necesarios.

La organización debería asegure que los recursos para la evaluación y el tratamiento del riesgo estén continuamente disponibles, para revisar los riesgos, para hacer frente a las amenazas o vulnerabilidades nuevas o modificadas, y para asesorar en adecuadamente a la dirección.

El seguimiento de la gestión del riesgo puede modificar o agregar al enfoque, metodología o herramientas utilizadas dependiendo de:

- los cambios identificados;

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- la iteración de la evaluación del riesgo;

- el objetivo del proceso de gestión del riesgo de seguridad de la información (por ejemplo, plan de continuidad del negocio, resiliencia a los incidentes, cumplimiento); y

- el objeto del proceso de gestión del riesgo de seguridad de la información (por ejemplo, organización, unidad de negocio, proceso de información, su implementación técnica, aplicación, conexión a Internet).

Salida: Relevancia continua del proceso de gestión del riesgo de seguridad de la información para los objetivos de negocio de la organización o la actualización del proceso.

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

ANEXO A
(INFORMATIVO)

Definición del alcance y límites del proceso de gestión del riesgo de seguridad de la información

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

A.1 Estudio de la organización

Estudio de la organización El estudio de la organización refiere a los elementos característicos que definen la identidad de una organización. Esto concierne al propósito, negocio, misiones, valores y estrategias de esta organización. Esto debería ser identificado junto con los elementos que contribuyan a su desarrollo (ejemplo subcontratación).

La dificultad de esta actividad reside en entender exactamente cómo está estructurada la organización. La identificación de su estructura real facilita la comprensión del rol y la importancia de cada división en el logro de los objetivos de la organización.

Por ejemplo, el hecho de que el oficial de seguridad de la información reporte a los altos directivos en lugar de a los gerentes de TI puede indicar la participación de los altos directivos en la seguridad de la información.

Objetivo principal de la organización: El objetivo principal de una organización puede ser definido como la razón por la que existe (su ramo de actividad, su segmento de mercado, entre otros).

Su negocio: El negocio de la organización, definido por las técnicas y el conocimiento (know-how) de sus empleados, le permite cumplir su misión. Esto es específico del ramo de actividad de la organización y a menudo define su cultura.

Su misión: La organización logra su propósito por el cumplimiento de su misión. Para identificar sus misiones, Los servicios prestados y/o los productos fabricados deberían ser identificados en relación con los usuarios finales.

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Sus valores: Los valores son principios fundamentales o un código de conducta bien definido que se aplica en el ejercicio del negocio. Estos pueden referirse al personal, las relaciones con agentes externos (clientes, entre otros), la calidad de los productos suministrados o servicios prestados.

Tomemos el ejemplo de una organización cuyo propósito es el servicio público, cuyo negocio es el transporte y cuya misión incluye el transporte de niños a/de la escuela. Sus valores pueden ser la puntualidad del servicio y la seguridad durante el transporte.

Estructura de la organización: Existen diferentes tipos de estructura:

- Estructura divisional: cada división se coloca bajo la autoridad de un director de la división responsable de las decisiones estratégicas, administrativas y operativas concernientes a su unidad.

- Estructura funcional: autoridad funcional es ejercida sobre los procedimientos, la naturaleza del trabajo y a veces sobre las decisiones o la planificación (por ejemplo, producción, TI, recursos humanos, marketing, entre otros).

Comentarios:

- Una división dentro de una organización con estructura divisional puede organizarse como una estructura funcional y viceversa

- Puede decirse que una organización tiene estructura matricial si tiene elementos de ambos tipos de estructura

- En cualquier estructura organizativa se pueden distinguir los siguientes niveles:

  - nivel de toma de decisiones (definición de orientaciones estratégicas);
  - nivel de liderazgo (coordinación y gestión); y
  - nivel operativo (producción y actividades de apoyo).

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Organigrama: La estructura de la organización se representa esquemáticamente en un organigrama. Esta representación debería destacar las líneas de reporte y la delegación de autoridad, pero es conveniente que también incluya otras relaciones, las cuales, aunque no sean sobre la base de ninguna autoridad formal, son sin embargo líneas de flujo de información.

La estrategia de la organización: Esto requiere una expresión formal de los principios rectores de la organización. La estrategia de la organización determina la dirección y el desarrollo necesarios a fin de beneficiarse de los elementos en juego y de los cambios más importantes que estén planificados.

A.2 Lista de las restricciones que afectan a la organización.

Todas las restricciones que afectan a la organización y que determinan su orientación hacia la seguridad de la información deberían ser tomadas en cuenta. Su fuente puede estar dentro de la organización, en cuyo caso tiene cierto control sobre ella o fuera de la organización y por tanto, generalmente, no negociable. Las restricciones de recursos (presupuesto, personal) y las restricciones de emergencia se encuentran entre las más importantes.

La organización establece sus objetivos (en relación con su negocio, comportamiento, entre otros) comprometiéndose a un determinado rumbo, posiblemente durante un largo período. Define lo que quiere llegar a ser y los medios que necesitarán implementarse. Al especificar este rumbo, la organización toma en cuenta la evolución de las técnicas y el conocimiento (know-how), los deseos expresados por los usuarios, clientes, entre otros. Este objetivo puede expresarse en la forma de estrategias operativas o de desarrollo con el objetivo, por ejemplo, de reducir los costos operativos, mejorar la calidad de servicio, entre otros.

Estas estrategias probablemente incluyen la información y el sistema de información (IS, por su sigla en inglés), que ayuda a su aplicación. En consecuencia, las características concernientes a la identidad, misión y estrategias de la organización son elementos fundamentales en el análisis del problema dado que la violación de un aspecto de seguridad de la información, podría dar lugar a repensar estos objetivos estratégicos. Además, es esencial que las propuestas para requisitos de seguridad de la información sigan siendo coherentes con las normas, usos y medios vigentes en la organización.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

La lista de restricciones incluye, pero no está limitada a:

- Restricciones de carácter político: Estas pueden referirse a las administraciones públicas, instituciones públicas o de manera más general, cualquier organización que tiene que aplicar decisiones del gobierno. En general son decisiones concernientes a la orientación estratégica u operativa establecidas por una división de gobierno o un órgano de toma de decisiones y se deberían aplicar.

  Por ejemplo, la informatización de las facturas o de documentos administrativos introduce problemas de seguridad de la información

- Restricciones de carácter estratégico: Las restricciones pueden surgir a partir de proyectos planificados o posibles cambios en las estructuras u orientación de la organización. Estas se expresan en la estrategia de la organización o en planes operativos.

  Por ejemplo, la cooperación internacional al compartir información sensible puede requerir acuerdos sobre intercambio seguro.

- Restricciones territoriales: La estructura de la organización y/o finalidad podrán introducir restricciones específicas, tales como la distribución de lugares en todo el territorio nacional o en el extranjero.

  Los ejemplos incluyen servicios postales, embajadas, bancos, filiales de un gran grupo industrial, entre otros.

- Restricciones derivadas del clima económico y político: Las operaciones de una organización puede ser profundamente cambiada por eventos específicos, tales como huelgas o crisis nacionales e internacionales.

  Por ejemplo, algunos servicios deberían ser capaces de continuar, incluso durante una grave crisis.

- Restricciones estructurales: La naturaleza de la estructura de una organización (divisional, funcional o de otro tipo) puede dar lugar a una política de seguridad de la información específica y a una organización de la seguridad adaptada a la estructura.

  Por ejemplo, una estructura internacional debería ser capaz de conciliar las necesidades de seguridad específicas para cada país.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- Restricciones funcionales: Restricciones funcionales se derivan directamente de las misiones generales o específicas de la organización.

  Por ejemplo, una organización que opera las veinticuatro horas del día debería asegurar que sus recursos se encuentran continuamente disponibles.

- Restricciones concernientes al personal: La naturaleza de estas restricciones varía considerablemente. Estas están relacionadas con: nivel de responsabilidad, contratación, calificación, formación, concientización sobre la seguridad, motivación, disponibilidad, entre otros.

  Por ejemplo, todo el personal de una organización de defensa debería tener autorización para manejar información altamente confidencial.

- Restricciones derivadas del calendario de la organización: Estas restricciones pueden ser resultado de la reestructuración o la creación de nuevas políticas nacionales o internacionales que impongan ciertos plazos.

  Por ejemplo, la creación de una división de seguridad.

- Restricciones relacionadas con los métodos: Tendrán que ser impuestos métodos adecuados al conocimiento (know-how) de la organización para aspectos tales como planificación de proyectos, especificaciones, desarrollo, entre otros.

  Por ejemplo, una típica restricción de este tipo es la necesidad de incorporar las obligaciones legales de la organización en la política de seguridad.

- Restricciones de naturaleza cultural: En algunas organizaciones los hábitos de trabajo o el negocio principal han dado lugar a una "cultura" específica dentro de la organización, la cual puede ser incompatible con los controles de seguridad. Esta cultura es el marco de trabajo de referencia del personal y puede ser determinada por muchos aspectos, incluida la educación, instrucción, experiencia profesional, experiencia fuera del trabajo, opiniones, filosofía, creencias, condición social, entre otros.

- Restricciones presupuestarias: Los controles de seguridad recomendados pueden tener a veces un costo muy alto. Aunque no siempre es conveniente basar la inversión en seguridad en la relación costo-beneficio, generalmente es requerida una justificación económica por parte del departamento financiero de la organización.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Por ejemplo, en el sector privado y algunos organismos públicos, el costo total de controles de seguridad no debe superar el costo de las posibles consecuencias de los riesgos. La alta dirección debería, por tanto, evaluar y tomar riesgos calculados si quieren evitar excesivos gastos de seguridad.

A.3 Lista de restricciones que afectan el alcance

Al identificar las restricciones es posible listar aquellas que tienen un impacto sobre el alcance y determinar no obstante cuáles son pasibles de acción. Estas se añaden, y pueden eventualmente modificar, las restricciones de la organización determinadas anteriormente. En los párrafos siguientes se presenta una lista no exhaustiva de posibles tipos de restricciones.

Restricciones derivadas de procesos pre-existentes

Los proyectos de aplicación no son necesariamente desarrollados simultáneamente. Algunos dependen de procesos pre-existentes. Incluso si un proceso puede dividirse en sub-procesos, el proceso no es necesariamente influenciado por todos los sub-procesos de otro proceso.

Restricciones técnicas

Restricciones técnicas, relacionadas con la infraestructura, generalmente surgen de instalar hardware y software, y de las salas o sitios donde se alojen los procesos de:

- archivos (requisitos en materia de organización, gestión de los medios, gestión de las normas de acceso, entre otros);
- arquitectura general (requisitos relativos a la topología (centralizada, distribuida, cliente-servidor), arquitectura física, entre otros);
- software de aplicación (en relación con las necesidades específicas de diseño de software, normas del mercado, entre otros);
- paquete de software (requisitos relativos a las normas, el nivel de valoración, calidad, cumplimiento de normas, seguridad, entre otros);

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- hardware (requisitos relativos a las normas, la calidad, el cumplimiento de las normas, entre otros);

- redes de comunicación (requisitos relativos a la cobertura, normas, capacidad, fiabilidad, entre otros); y

- infraestructura edificada (requisitos relativos a ingeniería civil, construcción, alto voltaje, bajo voltaje, entre otros).

Restricciones financieras

La implementación de controles de seguridad es a menudo restringida por el presupuesto que la organización puede comprometer. Sin embargo, las restricciones financieras deberían ser las últimas en ser consideradas para la asignación presupuestaria en seguridad, dado que se puede negociar sobre la base del estudio de seguridad.

Restricciones ambientales

Las restricciones ambientales surgen del entorno geográfico o económico en que los procesos se ejecutan: país, clima, riesgos naturales, situación geográfica, clima económico, entre otros.

Restricciones de tiempo

Se debería considerar el tiempo requerido para la implementación de controles de seguridad en relación con la capacidad para actualizar el sistema de información, si el tiempo de implementación es muy largo, los riesgos para los cuales el control fue diseñado pueden haber cambiado. El tiempo es un factor determinante para la selección de prioridades y soluciones.

Restricciones relacionadas con los métodos

Se debería utilizar métodos adecuados al conocimiento (know-how) de la organización para la planificación de proyectos, especificaciones, desarrollo y demás.

Restricciones de organización

Pueden surgir diversas restricciones a partir de los requisitos de organización:

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

- operación (requisitos relativos a los plazos, la oferta de servicios, vigilancia, seguimiento, planes de emergencia, operaciones degradadas, entre otros);

- mantenimiento (requisitos para la localización y solución de incidentes, acciones preventivas, correcciones rápidas, entre otros);

- gestión de los recursos humanos (requisitos relacionados con la formación de operarios y usuarios, calificación para puestos como administrador del sistema o administrador de datos, entre otros);

- gestión administrativa (requisitos relativos a las responsabilidades, entre otros);

- gestión del desarrollo (requisitos relativos a las herramientas de desarrollo, ingeniería de software asistida por computadora, planes de aceptación, organización a ser establecida, entre otros); y

- gestión de las relaciones exteriores (requisitos en materia de organización de relaciones con terceras partes, contratos, entre otros).

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

ANEXO B
(INFORMATIVO)

Identificación y evaluación de activos y evaluación de impacto

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

B.1 Ejemplos de identificación de activos

B.1.1 Generalidades

Para realizar una evaluación de activos, una organización necesita primero identificar sus activos (en un nivel de detalle apropiado). Se pueden distinguir dos tipos de activos:

- los activos primarios:
  - procesos y actividades del negocio;
  - información;
- los activos de soporte (de los cuales dependen los elementos primarios del alcance) de todo tipo:
  - hardware;
  - software;
  - redes;
  - personal;
  - sitio; y
  - estructura de la organización

B.1.2 Identificación de los activos primarios

Para describir el alcance con más precisión, esta actividad consiste en identificar los activos primarios (procesos y actividades del negocio, información). Esta identificación es llevada a cabo por un grupo de trabajo mixto representativo del proceso (gerentes, especialistas de los sistemas de información y usuarios).

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Los activos primarios son usualmente los procesos y la información esenciales de la actividad en el alcance. Pueden considerarse también otros activos primarios tales como los procesos de la organización, lo cual será más apropiado para elaborar una política de seguridad de la información o un plan de continuidad del negocio. Dependiendo del propósito, algunos estudios no requerirán de un análisis exhaustivo de todos los elementos que componen el alcance. En tales casos, los límites del estudio pueden ser limitados a los elementos clave del alcance.

Los activos primarios son de dos tipos:

1) Procesos del negocio (o sub-procesos) y actividades, por ejemplo:

   - procesos cuya pérdida o degradación hacen que sea imposible llevar a cabo la misión de la organización;
   - procesos que contienen procesos secretos o procesos que involucran tecnología propietaria;
   - procesos que, si se modifican, pueden afectar en gran medida el logro de la misión de la organización;
   - procesos que son necesarios para que la organización cumpla con requerimientos contractuales, legales o reglamentarios. Identificados en el capítulo 6;

2) Información. Generalmente, la información primaria comprende principalmente:

   - información vital para el ejercicio de la misión de la organización o el negocio;
   - información personal, tal como específicamente puede definirse en el sentido de las legislaciones nacionales respecto a la privacidad;
   - información estratégica necesaria para lograr los objetivos determinados por las orientaciones estratégicas; y
   - información de costo alto cuya recolección, almacenamiento, procesamiento y transmisión requieren mucho tiempo y/o implican un alto costo de adquisición.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Los procesos y la información que no están identificados como sensibles después de esta actividad no tendrán ninguna clasificación definida en el resto del estudio. Esto significa que incluso si tales procesos o información son comprometidos, la organización aún cumplirá la misión con éxito.

Sin embargo, a menudo heredarán controles implementados para proteger la información y los procesos identificados como sensibles.

B.1.3 Lista y descripción de los activos de apoyo

La meta consiste en que los activos sean identificados y descritos. Estos activos tienen vulnerabilidades que pueden ser explotadas por las amenazas destinadas a dañar los activos primarios del alcance definido (información y los procesos). Ellos son de varios tipos:

- Hardware. El tipo de hardware se compone de todos los elementos físicos de apoyo a los procesos.

  - Equipo de procesamiento de datos (activo): Equipo de procesamiento automático de información, incluidos los elementos requeridos para la operación independiente.

  - Equipo transportable: Equipo de cómputo portátil.

    Ejemplos: computadora portátil, Asistente Personal Digital (PDA, por su sigla en inglés).

  - Equipo fijo: Los equipos informáticos utilizados en las instalaciones de la organización.

    Ejemplos: servidores, micro-computadoras utilizadas como estación de trabajo.

  - Periféricos para procesamiento: Equipo conectado a una computadora mediante un puerto de comunicaciones (serie, paralelo, entre otros) para el ingreso, el transporte o la transmisión de datos.

    Ejemplos: impresora, unidad de disco extraíble.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- Medio de datos (pasivo): Estos son los medios para el almacenamiento de datos o funciones.

- medio electrónico: Un medio de información que puede ser conectado a una computadora o una red de computadoras para el almacenamiento de datos. A pesar de su tamaño compacto, estos medios pueden llegar a contener una gran cantidad de datos. Se pueden utilizar con un equipo informático estándar.

  Ejemplos: disquete, CD ROM, cartucho de respaldo, disco duro extraíble, memoria flash, cinta.

- otros medios: Estáticos, medios no electrónicos conteniendo datos.

  Ejemplos: papel, diapositiva, transparencia, documentación, fax.

- Software. El tipo Software está compuesto por todos los programas que contribuyen a la operación de un conjunto de procesamiento de datos.

  - Sistema operativo: Esto incluye todos los programas de una computadora que componen la base de operaciones a partir de la cual todos los demás programas (aplicaciones o servicios) son ejecutados. Incluye un núcleo y servicios o funciones básicas. Dependiendo de la arquitectura, un sistema operativo puede ser monolítico o construido a partir de un micro-núcleo y un conjunto de servicios del sistema. Los elementos principales del sistema operativo son todos los servicios de gestión del equipo (CPU, memoria, disco e interfaces de red), las tareas o servicios de gestión de procesos y los servicios de gestión de derechos de usuario.

  - Software de servicios, mantenimiento o administración: Software caracterizado por el hecho de complementar los servicios del sistema operativo y no está directamente al servicio de los usuarios o aplicaciones (aunque generalmente es esencial e incluso indispensable para el funcionamiento global del sistema de información).

  - Paquete de software o software estándar: Software estándar o paquete de software son los productos completos comercializados como tales (en lugar de desarrollos a medida o específicos) con soporte, liberación y mantenimiento. Proporcionan servicios a los usuarios y aplicaciones, pero no son personalizados o específicos como si lo pueden ser las aplicaciones del negocio.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Ejemplos: software de gestión de base de datos, software de mensajería electrónica, colaboración, software de directorio, software de servidor web, entre otros.

- Aplicaciones de negocio:

- Aplicaciones de negocio estándar: Se trata de un software comercial diseñado para dar a los usuarios acceso directo a los servicios y funciones que requieren de su sistema de información en su contexto profesional. Hay una muy amplia, teóricamente ilimitada, gama de campos.

  Ejemplos: software de contabilidad, software de control de maquinaria, software de atención al cliente, software de gestión de las competencias del personal, software administrativo, entre otros.

- Aplicaciones de negocio específicas: Este es software en el cual varios aspectos (principalmente soporte, mantenimiento, actualización, entre otros) han sido desarrollados específicamente para dar a los usuarios acceso directo a los servicios y funciones que requieren de su sistema de información. Hay una muy amplia, teóricamente ilimitada, gama de campos.

  Ejemplos: Gestión de la facturación a los clientes de los operadores de telecomunicaciones, seguimiento en tiempo real de la aplicación para el lanzamiento de cohetes.

- Red: El tipo red se compone de todos los dispositivos de telecomunicaciones utilizados para interconectar varias computadoras físicamente remotas o elementos de un sistema de información.

  Ejemplos: Red Telefónica Pública (PSTN - Public Switching Telephone Network), Ethernet, Gigabit Ethernet, Asymmetric Digital Subscriber Line (ADSL), especificaciones de protocolo inalámbrico (por ejemplo, WiFi 802.11), Bluetooth, FireWire.

- Medio y soporte: Los medios o equipos de comunicaciones y telecomunicaciones son caracterizados principalmente por las características físicas y técnicas de los equipos (punto a punto, broadcast) y por los protocolos de comunicación (enlace o red - niveles 2 y 3 del modelo OSI de 7 capas).

- Retransmisión (relay) pasiva o activa: Este sub-tipo incluye todos los dispositivos que no son terminaciones lógicas de las comunicaciones (visión de Seguridad de la Información), pero son dispositivos intermedios o de

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

retransmisión (relay). Las retransmisiones (relays) se caracterizan por los protocolos de comunicación de red soportados. Además de la retransmisión básica, a menudo incluyen routing y / o funciones de filtrado y servicios, empleando conmutadores (switches) de comunicación y routers con filtros. A menudo pueden ser administrados a distancia y por lo general son capaces de generar logs.

Ejemplos: bridge, router, hub, switch, intercambio automático.

- Interfaz de comunicación: Las interfaces de comunicación de las unidades de procesamiento están conectadas a las unidades de procesamiento pero se caracterizan por los medios y los protocolos de soporte, por cualquier filtrado instalado, registro (log) o funciones de generación de alertas y sus capacidades y por la posibilidad y necesidad de administración remota.

  Ejemplos: General Packet Radio Service C (GPRS), adaptador Ethernet.

- Personal: El tipo personal se compone de todos los grupos de personas involucradas en el sistema de información.

  - Tomadores de decisión: Los tomadores de decisiones son los propietarios de los activos primarios (información y funciones) y los directivos de la organización o de proyectos específicos.

    Ejemplos: alta dirección, jefe de proyecto.

  - Usuarios: Los usuarios son el personal que maneja elementos sensibles en el contexto de su actividad y que tienen una responsabilidad especial en este sentido. Ellos pueden tener derechos de acceso especiales al sistema de información para llevar a cabo sus tareas diarias.

    Ejemplos: gestión de recursos humanos, gestión financiera, gestor de riesgos.

  - Personal de operación/mantenimiento: Estos son el personal encargado de operar y mantener el sistema de información. Ellos tienen derechos de acceso especiales al sistema de información para llevar a cabo sus tareas diarias.

    Ejemplos: administrador del sistema, administrador de datos, operador de respaldos, mesa de ayuda, operador de la implantación de la aplicación, oficiales de seguridad.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- Desarrolladores: Los desarrolladores están a cargo de desarrollar las aplicaciones de la organización. Tienen acceso a una parte del sistema de información con alto nivel de derechos, pero no toman ninguna acción sobre los datos de producción.

  Ejemplos: desarrolladores de aplicaciones del negocio.

- Sitio: El tipo sitio comprende todos los lugares abarcados por el alcance o parte del mismo, y los medios físicos requeridos para su operación.

  - Ubicación:

  - Entorno externo: Esto afecta a todas las ubicaciones en las cuales los medios de seguridad de la organización no se pueden aplicar.

    Ejemplos: los hogares del personal, los locales de otra organización, el entorno fuera de la ubicación (área urbana, área de peligro).

  - Locales: Este lugar está limitado por el perímetro de la organización en contacto directo con el exterior. Esto puede ser una frontera física de protección obtenida mediante la creación de barreras físicas o medios de vigilancia alrededor de los edificios.

    Ejemplos: establecimientos, edificios.

  - Zona: Una zona está formada por una frontera física de protección que forma particiones dentro de las instalaciones de la organización. Se obtiene mediante la creación de barreras físicas en torno a las infraestructuras de procesamiento de la información de la organización.

    Ejemplos: oficinas, zona de acceso reservado, zona segura.

  - Servicios esenciales: Todos los servicios requeridos para que el equipamiento de la organización opere.

  - Comunicación: Los servicios y equipamiento de telecomunicaciones proporcionado por un operador.

    Ejemplos: líneas telefónicas, centralitas, redes telefónicas internas.

  - Utilitarios:

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- Servicios y medios (fuentes y cableado) requeridos para proporcionar energía al equipamiento y a los periféricos de tecnología de la información.

  Ejemplos: alimentación de baja tensión, inversor, circuito eléctrico head-end.

- Abastecimiento de agua

- Eliminación de residuos

- Servicios y medios (equipamiento, control) para la refrigeración y purificación del aire.

  Ejemplos: tuberías de agua refrigerada, acondicionadores de aire.

- Organización. El tipo organización describe el marco de trabajo organizacional, consistente en todas las estructuras de personal asignadas a una tarea y los procedimientos de control de estas estructuras.

- Autoridades: Se trata de organizaciones de las cuales las organizaciones estudiadas derivan su autoridad. Pueden ser legalmente afiliados o externas. Estas imponen limitaciones en la organización estudiada en términos de reglamentos, decisiones y acciones.

  Ejemplos: cuerpo de administración, Casa matriz de una organización.

- Estructura de la organización: Este consiste en las diversas ramas de la organización, incluida sus actividades transversales, bajo el control de su gestión.

  Ejemplos: gestión de recursos humanos, gestión de TI, gestión de compras, gestión de unidades de negocio, servicio de seguridad de los edificios, servicios de bomberos, gestión de auditorías.

- Proyecto u organización del sistema: Esto se refiere a la organización creada para un determinado proyecto o servicio.

  Ejemplos: proyecto de desarrollo de nueva aplicación, proyecto de migración de sistema de información.

- Subcontratistas/proveedores/fabricantes: Estas son organizaciones que proveen a la organización de un servicio o recurso y está vinculado a ella por contrato.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Ejemplos: compañía que gestiona las instalaciones, empresa subcontratada, empresas de consultoría.

B.2 Evaluación de activos

B.2.1 Generalidades

El siguiente paso después de la identificación del activo es llegar a un acuerdo sobre la escala que se utilizará y los criterios para la asignación de un lugar en esa escala para cada activo, sobre la base de valoración. Debido a la diversidad de los activos encontrados en la mayoría de las organizaciones es probable que algunos activos que tienen un valor monetario conocido se valorarán en la unidad local de moneda, mientras que otros que tienen un valor más cualitativo se le pueden asignar un valor que va, por ejemplo, de "muy bajo" a "muy alto". La decisión de utilizar una escala cuantitativa versus una escala cualitativa es realmente una cuestión de preferencia de la organización, pero que debería ser pertinente para los activos objeto de valoración. Ambos tipos de valoración podrían utilizarse para el mismo activo.

Términos típicos utilizados para la valoración cualitativa de los activos incluyen palabras tales como: insignificante, muy bajo, bajo, medio, alto, muy alto, y crítico. La elección y la variedad de términos adecuados para una organización dependen fuertemente de las necesidades de la organización en seguridad, del tamaño de la organización y otros factores específicos de la organización.

B.2.2 Criterios

Los criterios utilizados como base para asignar un valor a cada activo deberían ser escritos en términos inequívocos. Esto es a menudo uno de los aspectos más difíciles de la evaluación de activos ya que los valores de algunos activos pueden tener que ser determinados subjetivamente y que muchas personas diferentes sean quienes probablemente tomen la determinación. Posibles criterios utilizados para determinar el valor del activo incluyen su costo original, su costo de sustitución o de re-creación o su valor puede ser abstracto, por ejemplo, el valor de la reputación de una organización.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Otra base para la evaluación de los activos es el gasto debido a la pérdida de confidencialidad, integridad y disponibilidad como consecuencia de un incidente. se debería considerar también, no repudio, rendiciones de cuenta, autenticidad y fiabilidad, según corresponda. Esta valoración " sería un elemento importante para dimensionar el valor del activo, además del costo de reposición, basado en estimaciones de las consecuencias adversas para el negocio, producto de incidentes de seguridad con una supuesta serie de circunstancias. Se hace hincapié en que este enfoque tiene en cuenta las consecuencias que son necesarias considerar en la evaluación de riesgos.

Muchos activos durante el curso de la valoración pueden tener varios valores asignados. Por ejemplo: un plan de negocios puede tener un valor basado en el trabajo empleado en el desarrollo del plan, podría ser valorado en base al trabajo para introducir los datos, y puede ser valorado en base al valor para un competidor. Cada uno de los valores asignados probablemente difiera considerablemente.

El valor asignado puede ser el máximo de todos los valores posibles o puede ser la suma de todos o algunos de los posibles valores. En última instancia, qué valor o valores se asignan a un activo debería ser cuidadosamente determinado ya que el valor final asignado entra en la determinación de los recursos que se gastarán para la protección de los activos.

B.2.3 Reducción a una base común

En última instancia, todas las valoraciones de activos deben reducirse a una base común. Esto puede llevarse a cabo con la ayuda de criterios tales como los que siguen. Criterios que pueden utilizarse para evaluar las posibles consecuencias derivadas de una pérdida de confidencialidad, integridad, disponibilidad, no repudio, responsabilidad (accountability), autenticidad, o fiabilidad de los activos son los siguientes:

- deterioro de los resultados empresariales;
- pérdida de reputación / efecto negativo sobre la reputación;
- incumplimiento relacionado con información personal;
- peligro de la seguridad personal;
- efectos adversos sobre la aplicación de la ley;

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- incumplimiento de la confidencialidad;
- incumplimiento del orden público;
- pérdida financiera;
- interrupción a las actividades comerciales; y
- peligro de la seguridad ambiental.

Otro enfoque para evaluar las consecuencias podría ser:

- interrupción del servicio: imposibilidad de prestar el servicio;
- pérdida de la confianza de los clientes:
  - pérdida de credibilidad en el sistema de información interna; y
  - daños a la reputación;
- alteración del funcionamiento interno:
  - perturbación en la propia organización; y
  - costo adicional interior;
- alteración del funcionamiento de una tercera parte:
  - interrupción en transacciones de terceros con la organización; y
  - diversos tipos de daños;
- peligro para la seguridad del personal/usuario: peligro para el personal de la organización y/o usuarios;
- ataque a la vida privada de los usuarios;
- pérdidas financieras;
- costos financieros de emergencia o reparación:

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

  - en términos de personal;
  - en términos de equipamiento; y
  - en términos de estudios, informes de expertos;
- pérdida de bienes/fondos/activos;
- pérdida de clientes, pérdida de proveedores;
- procesos judiciales y penas;
- pérdida de una ventaja competitiva;
- pérdida de avances tecnológicos/técnicos;
- pérdida de eficacia/confianza;
- pérdida de reputación técnica;
- debilitamiento de la capacidad de negociación;
- crisis industrial (huelgas);
- crisis de gobierno;
- despido; y
- daños materiales.

Estos criterios son ejemplos de elementos que deben considerarse para la evaluación de activos. Para llevar a cabo valoraciones, una organización necesita seleccionar los criterios pertinentes a su tipo de negocio y los requisitos de seguridad. Esto podría significar que algunos de los criterios antes mencionados no son aplicables, y que tal vez otros tendrían que ser añadidos a la lista.

B.2.4 Escala

Después de establecer los criterios a ser considerados, la organización debería lleguar a un acuerdo sobre la escala que utilizará en toda la organización. El primer paso es decidir el

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

número de niveles que deben utilizarse. No hay reglas con respecto al número de niveles más adecuado. Más niveles proporcionan un mayor nivel de granularidad, pero a veces también una diferenciación muy fina hace difícil las decisiones coherentes a lo largo de la organización. Normalmente, cualquier número de niveles entre 3 (por ejemplo, bajo, medio y alto) y 10 se puede utilizar en tanto sea coherente con el enfoque que la organización está utilizando para todo el proceso de evaluación de riesgos.

Una organización puede definir sus propios límites para el valor de los activos, como ser "bajo", "medio", o "alto". se debería que estos límites sean evaluados de acuerdo con los criterios seleccionados (por ejemplo, para una posible pérdida financiera, se debería dar valores monetarios, pero para consideraciones tales como la puesta en peligro de la seguridad personal, las valoraciones monetarias pueden ser complejas y pueden no ser apropiados para todas las organizaciones). Por último, depende totalmente de la organización decidir qué se considera una consecuencia "baja" o "alta". Una consecuencia que podría ser desastrosa para una organización pequeña puede ser baja o incluso insignificante para una gran organización.

B.2.5 Dependencias

Cuanto más relevantes y numerosos son los procesos de negocio apoyados por un activo, mayor es el valor de este activo. se debería identificar dependencias de activos en los procesos de negocio y otros activos ya que esto podría influir en los valores de los activos. Por ejemplo, se debería mantener la confidencialidad de los datos a lo largo de su ciclo de vida, en todas las etapas, incluyendo el almacenamiento y procesamiento, es decir, las necesidades de seguridad de almacenamiento de datos y procesamiento de los programas deberían estar directamente relacionadas con el valor que representa la confidencialidad de los datos almacenados y procesados. Además, se debería que, si un proceso de negocio depende de la integridad de ciertos datos que se producen por un programa, los datos de entrada de este programa tengan la adecuada confiabilidad. Por otra parte, la integridad de la información dependerá del hardware y software utilizados para su almacenamiento y procesamiento. Asimismo, el hardware dependerá de la fuente de alimentación y posiblemente del aire acondicionado. Por lo tanto, la información sobre las dependencias ayudará en la identificación de amenazas y en particular vulnerabilidades. Además, contribuirá a asegurar que se da el verdadero valor a los activos (a través de las relaciones de dependencia), lo que indica el nivel apropiado de protección.

Los valores de los activos de los que dependen otros activos podrán ser modificados de la siguiente manera:

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- Si los valores de los activos dependientes (por ejemplo, los datos) son inferiores o iguales al valor del bien considerado (por ejemplo, software), su valor sigue siendo el mismo;

- se debería que si los valores de los activos dependientes (por ejemplo, los datos) son mayores, entonces el valor de los activos considerados (por ejemplo, software) aumente de acuerdo a:

  - El grado de dependencia; y
  - Los valores de los otros activos.

Una organización puede tener algunos activos que estén disponibles más de una vez, como ser copias de programas informáticos o el mismo tipo de computadora utilizado en la mayoría de las oficinas. Es importante tener en cuenta este hecho cuando se hace la evaluación de activos. Por un lado, estos activos son fácilmente pasados por alto, por lo que se debería tener cuidado en identificar todos ellos; por otro lado, podrían ser utilizados para reducir los problemas de disponibilidad.

B.2.6 Salida

La salida final de este paso es una lista de activos y su valor en relación con la divulgación (preservación de la confidencialidad), modificación (preservación de la integridad, autenticidad, no repudio y responsabilidad (accountability)), la no-disponibilidad y la destrucción (la preservación de la disponibilidad y fiabilidad), y el costo de reposición.

B.3 Evaluación del impacto

Un incidente de seguridad de la información puede afectar a más de un activo o sólo una parte de un activo. El impacto se relaciona con el grado de éxito del incidente. Como consecuencia de ello, existe una diferencia importante entre el valor del activo y el impacto causados por el incidente. Se considerará impacto ya sea de efecto inmediato (operacional) o de efecto futuro (negocio) que incluye consecuencias financieras y de mercado.

El impacto inmediato (operacional) es tanto directo como indirecto.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

1) Directo:

   a) el valor financiero de reposición por la pérdida del activo (o parte del activo);

   b) el costo de adquisición, configuración e instalación del nuevo activo o respaldo;

   c) el costo de las operaciones suspendidas debido al incidente hasta que el servicio proporcionado por el activo(s) es restaurado; y

   d) el impacto se traduce en una brecha de seguridad de la información.

2) Indirecto:

   a) costo de oportunidad (los recursos financieros necesarios para reemplazar o reparar un activo se habrían utilizado en otros lugares);

   b) costo de la interrupción de las operaciones;

   c) potencial uso indebido de la información obtenida a través de una brecha de seguridad;

   d) violación de las obligaciones reglamentarias o estatutarias; y

   e) violación de los códigos de conducta ética.

Como tal, la primera valoración (sin controles de ningún tipo) estimará un impacto muy cerca al valor (o combinación de los valores) del activo(s) involucrado(s). En una próxima iteración de este(estos) activo(s), el impacto será diferente (por lo general mucho más bajo) debido a la presencia y la eficacia de los controles implementados.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

ANEXO C
(INFORMATIVO)

Ejemplos de amenazas típicas

La tabla siguiente muestra ejemplos de amenazas típicas. Se puede utilizar la lista durante el proceso de evaluación de la amenaza. Las amenazas pueden ser deliberadas, accidentales o ambientales (naturales) y pueden resultar, por ejemplo, en daño o pérdida de servicios esenciales. La lista siguiente indica para cada tipo de amenaza donde D (deliberada), A (accidental), E (ambiental) es relevante. D se utiliza para toda acción deliberada que apunte a los activos de información, A se utiliza para toda acción humana que accidentalmente pueda dañar activos de información, y se utiliza para todos los incidentes que no se basen en acciones humanas. Los grupos de amenazas no están en orden de prioridad.

Tipo	Amenazas	Origen
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Incidente importante	A, D, E
	Destrucción de equipamiento o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómeno climático	E
	Fenómenos sísmicos	E
	Fenómeno volcánico	E
	Fenómeno meteorológico	E
	Inundación	E
Pérdida de servicios esenciales	Falla de aire acondicionado o sistema de suministro de agua	A, D
	Pérdida de suministro de energía	A, D, E
	Falla de equipamiento de telecomunicaciones	A, D, E
Perturbación debida a radiación	Radiación electromagnética	A, D, E
	Radiación térmica	D
	Pulsos electromagnéticos	D

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Tipo	Amenazas	Origen
Compromiso de información	Interceptación de señales de interferencias comprometidas	D
	Espionaje remoto	D
	Escucha secreta	D
	Robo de medios o documentos	D
	Robo de equipos	D
	Recuperación de medios reciclados o descartados	D
	Divulgación	A, D
	Datos de fuentes poco fiables	A, D
	Manipulación (tampering) con hardware	D
	Manipulación (tampering) con software	A, D
	Detección de posición	D
Fallas técnicas	Falla de equipo	A
	Mal funcionamiento de equipo	A
	Saturación de sistema de información	A, D
	Mal funcionamiento de software	A
	Brecha/fisura de mantenimiento de sistema de información	A, D
Acciones no autorizadas	Uso no autorizado de equipo	D
	Copia fraudulenta de software	D
	Uso de software falsificado o copiado	A, D
	Corrupción de datos	D
	Procesamiento ilegal de datos	D
Compromiso de funciones	Error en uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Brecha de disponibilidad de personal	A, D, E

Se debería prestar particular atención a las fuentes de amenaza humana. Estas se detallan específicamente en la siguiente tabla:

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Fuente de amenaza	Motivación	Acciones de amenaza
Hacker, cracke	Desafío Ego Rebelión Estatus Dinero	- Hacking - Ingeniería social - Intrusión de Sistema, irrupciones - Acceso no autorizado a sistema
Delito informático	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de datos	- Delito informático (por ejemplo, acoso cibernético) - Acto fraudulento (por ejemplo, repetición, personificación, interceptación) - Soborno de información - Engaño - Intrusión de sistemas
Terrorista	Chantaje Destrucción Explotación Venganza Ganancia política Cobertura mediática	- Bomba/Terrorismo - Guerra de información - Ataque de sistema (por ejemplo, negación distribuida de servicio) - Penetración de sistema - Manipulación (tampering) de sistema
Espionaje industrial (Inteligencia, compañías, gobiernos extranjeros, otros intereses del gobierno)	Ventaja competitiva Espionaje económico	- Ventaja de Defensa - Ventaja Política - Explotación económica - Robo de información - Intrusión en privacidad personal - Ingeniería social - Penetración de sistema - Acceso no autorizado al sistema (acceso a información clasificada, propietaria, y/o relacionada con tecnología)
Internos (empleados pobremente entrenados, descontentos, maliciosos, negligentes, deshonestos, o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (Por ejemplo, error de entrada de datos, error de programación)	- Asalto a un empleado - Chantaje - Mirada a información propietaria - Abuso de computadora - Fraude y robo - Soborno de información - Entrada de datos falsificados, corruptos - Interceptación - Código malicioso (Por ejemplo, virus, bomba lógica, caballo de Troya) - Venta de información personal - Errores de sistema - Intrusión de sistema - Sabotaje de sistema - Acceso no autorizado a sistema

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

ANEXO D
(INFORMATIVO)

Vulnerabilidades y métodos para evaluación de vulnerabilidades

PROHIBIDA LA REPRODUCCIÓN TOTAL O PARCIAL

D.1 Ejemplos de vulnerabilidades

La tabla siguiente da ejemplos de vulnerabilidades en varias áreas de seguridad, incluyendo ejemplos de amenazas que podrían explotar estas vulnerabilidades. Las listas pueden proveer ayuda durante la evaluación de amenazas y vulnerabilidades, para determinar escenarios de incidentes relevantes. Se enfatiza que en algunos casos también otras amenazas pueden explotar estas vulnerabilidades.

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de esquemas periódicos de reemplazo	Destrucción de equipo o medios
	Susceptibilidad a humedad, Polvo, corrosión,	Polvo, suciedad, congelamiento
	Sensibilidad a radiación electromagnética	Radiación electromagnética
	Falta de control eficiente de cambio de configuración	Error en uso
	Susceptibilidad a variaciones de voltaje	Pérdida de suministro de voltaje
	Susceptibilidad a variaciones de temperatura	Fenómeno meteorológico
	Almacenamiento no protegido	Robo de medios o documentos
	Falta de cuidado en eliminación	Robo de medios o documentos
	Copiado no controlado	Robo de medios o documentos
Software	Falta o insuficiente prueba de software	Abuso de derechos
	Fallas bien conocidas en el software	Abuso de derechos
	No se cierra la sesión cuando se abandona la estación de trabajo	Abuso de derechos

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Eliminación o reutilización de medios de almacenamiento sin borrado apropiado	Abuso de derechos
	Falta de seguimiento de auditoría	Abuso de derechos
	Incorrecta asignación de derechos de acceso	Abuso de derechos
	Software ampliamente distribuido	Corrupción de datos
	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	Corrupción de datos
	Complicada interfase de usuario	Error en uso
	Falta de documentación	Error en uso
	Establecer parámetros incorrectos	Error en uso
	Fechas incorrectas	Error en uso
	Falta de mecanismos de identificación y autenticación como autenticación de usuario	Falsificación de derechos
	Tablas de contraseñas no protegidas	Falsificación de derechos
	Manejo / pobre de contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento de Software
	Especificaciones poco claras o incompletas para desarrolladores	Mal funcionamiento de Software
	Falta de control de cambio efectivo	Mal funcionamiento de Software
	Descarga y uso no controlado de software	Manipulación (tampering) con software
	Falta de copias de respaldo	Manipulación (tampering) con software
	Falta de protección física del edificio, puertas y ventanas	Robo de medios o documentos
	Falla en producir reportes de gestión	Uso no autorizado de equipos
Red	Falta de prueba de envío o recepción de un mensaje	Negación de acción
	Líneas de comunicación desprotegidas	Escucha (Eavesdropping)

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Tráfico sensible desprotegido	Escucha (Eavesdropping)
	Pobre conjunto de cableado	Falla en el equipo de telecomunicaciones
	Punto único de falla	Falla en el equipo de telecomunicaciones
	Falta de identificación y autenticación del remitente y el receptor	Falsificación de derechos
	Inseguridad en la arquitectura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Inadecuada gestión de red (Resiliencia de ruteo)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado de equipos
Personal	Ausencia de personal	Brecha de disponibilidad de personal
	Procedimientos inadecuados de reclutamiento	Destrucción de equipamiento o medios
	Entrenamiento insuficiente en seguridad	Error en uso
	Uso incorrecto de software y hardware	Error en uso
	Falta de conciencia de seguridad	Error en uso
	Falta de mecanismos de seguimiento	Procesamiento ilegal de datos
	Trabajo no supervisado por personal externo o de limpieza	Robo de medios o documentos
	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	Uso no autorizado de equipamiento
Local	Uso inadecuado o descuidado de control de acceso físico a edificios y recintos	Destrucción de equipamiento o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red de energía inestable	Pérdida de suministro de energía
	Falta de protección física del edificio, puertas y ventanas	Robo de equipamiento
	Falta de procedimiento formal para registro de usuarios y su baja	Abuso de derechos

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Falta de proceso formal para revisión de derechos de acceso (supervisión)	Abuso de derechos
	Falta o insuficientes capítulos (concernientes a seguridad) en contratos con clientes y/o terceros	Abuso de derechos
	Falta de procedimiento de seguimiento de instalaciones de procesamiento de la información	Abuso de derechos
Organización	Falta de auditorías regulares (supervisión)	Abuso de derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de derechos
	Falta de reportes de fallas registrados en bitácoras del administrador y operador	Abuso de derechos
	Respuesta inadecuada de mantenimiento de servicio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta o insuficiente Acuerdo de Nivel de Servicio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de procedimiento de control de cambio	Brecha en la capacidad de mantenimiento del sistema de información
	Falta de procedimiento formal para control de la documentación del SGSI	Corrupción de datos
	Falta de procedimiento formal para la supervisión de los registros del SGSI	Corrupción de datos
	Falta de proceso formal para autorización de información públicamente disponible	Datos de fuentes no confiables
	Falta de asignación apropiada de responsabilidades por la seguridad de la información	Negación de acciones
	Falta de planes de continuidad	Falla de equipamiento
	Falta de política de uso de e-mail	Error en uso
	Falta de procedimientos para introducir software a sistemas operacionales	Error en uso

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Falta de registros en bitácoras del administrador y operador	Error en uso
	Falta de procedimientos para manejo de información clasificada	Error en uso
	Falta de responsabilidades de seguridad de la información en descripciones de puestos	Error en uso
	Falta o insuficientes estipulaciones (concernientes a seguridad de la información) en contratos con empleados	Procesamiento de datos ilegal
	Falta de proceso disciplinario definido en caso de incidente de seguridad de la información	Robo de equipamiento
	Falta de política formal sobre uso de computadoras móviles	Robo de equipamiento
	Falta de control de activos fuera de las instalaciones	Robo de equipamiento
	Falta o insuficiente política de escritorio y pantalla limpia	Robo de medios o documentos
	Falta de autorización a las instalaciones de procesamiento de la información	Robo de medios o documentos
	Falta de mecanismos de seguimiento establecidos para brechas de seguridad	Robo de medios o documentos
	Falta de revisiones regulares de gestión	Uso no autorizado de equipamiento
	Falta de procedimientos para reportar debilidades de la seguridad	Uso no autorizado de equipamiento
	Falta de procedimientos de estipulación de cumplimiento con derechos de propiedad intelectual	Uso de software falso o copiado

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

D.2 Métodos para la valoración técnica de vulnerabilidades

Métodos proactivos tales como evaluaciones del sistema de información pueden utilizarse para identificar las vulnerabilidades en función de la criticidad de los sistemas y de los recursos disponibles de Tecnologías de Información y de Comunicaciones (TIC) (por ejemplo, los fondos asignados, la tecnología disponible, las personas con los conocimientos necesarios para realizar la prueba). Los métodos de prueba incluyen:

- herramientas automatizadas de escaneo de vulnerabilidad;
- pruebas y evaluaciones de seguridad;
- pruebas de penetración; y
- revisión de código

La herramienta automatizada de escaneo de vulnerabilidad se utiliza para escanear un grupo de equipos (hosts) o una red para conocer los servicios vulnerables (por ejemplo, el sistema permite File Transfer Protocol (FTP) anónimo, transmisión de envío de mail). Cabe señalar, sin embargo, que algunas de las posibles vulnerabilidades identificadas por la herramienta automatizada de escaneo podrían no representar vulnerabilidades reales en el contexto del entorno del sistema. Por ejemplo, algunas de estas herramientas de escaneo tasan potenciales vulnerabilidades, sin considerar el entorno y los requisitos. Algunas de las vulnerabilidades marcadas por el software de escaneo automatizado pueden actualmente no ser vulnerables en un entorno determinado, pero pueden estar configuradas de esta manera porque su entorno así lo requiere. Por lo tanto, este método puede producir falsos positivos.

Evaluación y pruebas de seguridad (STE, por su sigla en inglés) es otra técnica que puede utilizarse para identificar las vulnerabilidades de un sistema de TIC durante el proceso de evaluación de riesgos. Incluye la elaboración y ejecución de un plan de pruebas (por ejemplo, secuencia de comandos de prueba, procedimientos de prueba, y los resultados esperados de la prueba). El objetivo de la prueba de seguridad del sistema es probar la eficacia de los controles de seguridad de un sistema de TIC, como se hubiesen aplicado en el entorno de operaciones. El objetivo es garantizar que los controles aplicados satisfacen las especificaciones de seguridad aprobadas para el software y hardware e implementan la política de seguridad de la organización o cumple con las normas de la industria.

PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

La prueba de penetración puede utilizarse para complementar la revisión de los controles de seguridad y garantizar que las diferentes facetas del sistema de las TIC son seguras. La prueba de penetración, cuando se utiliza en el proceso de evaluación de riesgos, puede utilizarse para evaluar la capacidad del sistema de TIC de resistir los intentos intencionales de eludir la seguridad del sistema. Su objetivo es poner a prueba el sistema de TIC desde la perspectiva de una fuente de amenaza para identificar las posibles fallas en el esquema de protección del sistema de TIC.

La revisión de código es el más profundo (pero también el más caro) camino de evaluación de vulnerabilidad.

Los resultados de estos tipos de pruebas de seguridad ayudarán a identificar las vulnerabilidades de un sistema.

Es importante notar que las herramientas y técnicas de penetración pueden dar resultados falsos a menos que la vulnerabilidad sea explotada exitosamente. Para explotar vulnerabilidades en particular se debe conocer la configuración del sistema / la aplicación / parches exacta en el sistema probado. Si estos datos no son conocidos en el momento de la prueba, puede no ser posible explotar exitosamente una vulnerabilidad en particular (por ejemplo, obtener una sesión de comandos en el sistema remoto); sin embargo, es posible hacer fallar o reiniciar un proceso o sistema de prueba. En tal caso, se debería que el objeto probado sea también considerado vulnerable.

Los métodos pueden incluir las siguientes actividades:

- entrevistar personas o usuarios;
- cuestionarios;
- inspección física; y
- análisis de documento.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

ANEXO E
(INFORMATIVO)

Enfoques a la evaluación del riesgo de seguridad de la información

E.1 Evaluación del riesgo de seguridad de la información de alto nivel

La evaluación de alto nivel permite la definición de prioridades y cronología en las acciones. Por varias razones, tales como el presupuesto, puede no ser posible implementar todos los controles simultáneamente y solamente pueden ser manejados durante el proceso de tratamiento del riesgo aquellos más críticos. También, puede ser prematuro comenzar un análisis del riesgo detallado si la implementación se avizora después de uno o dos años. Para alcanzar este objetivo, la evaluación de alto nivel puede comenzar con una evaluación de alto nivel de las consecuencias en lugar de comenzar con un sistemático análisis de amenazas, vulnerabilidades, activos y consecuencias.

Otra razón para comenzar con una evaluación de alto nivel es sincronizar con otros planes relacionados al manejo de cambios (o continuidad de negocio). Por ejemplo, no suena lógico asegurar un sistema completamente si se planea tercerizarlo en un futuro cercano, si bien puede ser de valor hacer la evaluación de riesgo con el objetivo de definir el contrato de tercerizacíón.

Las características de la evaluación del riesgo de alto nivel podrían incluir lo siguiente:

- La evaluación del riesgo de alto nivel podrá dirigir una visión I global de la organización, considerando los aspectos tecnológicos como independientes de los de negocio. Haciendo esto, el contexto de análisis se concentra más en los ambientes de negocio y operativo que en los elementos tecnológicos.

- La evaluación del riesgo de alto nivel podrá tratar un número limitado de amenazas, y vulnerabilidades agrupadas en distintos dominios o, para agilizar el proceso, puede focalizar en escenarios del riesgo o ataques en lugar de en sus elementos.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- Los riesgos presentados en la evaluación del riesgo de alto nivel son frecuentemente dominios de riesgo más generales que los riesgos identificados específicamente. Como los escenarios y riesgos están agrupados en dominios, el proceso de tratamiento del riesgo lista los controles en cada dominio. Las actividades de tratamiento del riesgo intentan primero proponer y seleccionar controles comunes que sean válidos a lo largo de todo el sistema.

- Sin embargo, la evaluación del riesgo de alto nivel, debido a que rara vez incluye detalles tecnológicos, es más apropiada para proveer controles organizacionales y no técnicos y gestionar aspectos de los controles técnicos, o salvaguardas técnicas claves y comunes tales como respaldos y antivirus.

Las ventajas de la evaluación del riesgo de alto nivel son las siguientes:

- La incorporación de una aproximación inicial simple es probablemente como ganar la aceptación del programa de valoración.

- Debería ser posible construir una imagen de la estrategia del programa de seguridad de la organización, es decir va a actuar como una buena ayuda para la planificación.

- Recursos y dinero pueden ser aplicados donde sea más beneficioso, y los sistemas que necesiten la mayor protección van a ser atendidos primero.

Como el análisis inicial es de alto nivel, y potencialmente menos exacto, la única posible desventaja es que algunos procesos de negocio o sistemas podrían no ser identificados los cuales requerirían una segunda y detallada evaluación de riesgo. Esto podría ser evitado si se dispone de información en todos los aspectos de la organización y sus sistemas, incluyendo información obtenida en la evaluación de incidentes de seguridad.

La evaluación del riesgo de alto nivel considera el valor para el negocio de los activos, y los riesgos desde el punto de vista de negocio de la organización. En el primer punto de decisión (véase Figura 2), varios factores asisten en determinar si la evaluación de alto nivel es adecuada para el tratamiento de los riesgos; estos factores podrían incluir lo siguiente:

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- los objetivos de negocio a ser alcanzados utilizando varios activos de información;

- el grado en que los negocios de la organización dependen de cada activo de información, es decir si las funciones que la organización considera críticas para su supervivencia o la conducción efectiva del negocio son dependientes de cada activo, o de la confidencialidad, integridad, disponibilidad, no repudio, responsabilidad, autenticidad, y confiabilidad de la información almacenada y procesada por ese activo;

- el nivel de inversión en cada activo de información, en términos de desarrollo, mantenimiento, reemplazo del activo; y

- el activo de información, para los cuales la organización directamente asigna un valor.

Cuando estos factores son tratados, la decisión se vuelve fácil. Si el objetivo de un activo es extremadamente importante para la conducción de los negocios de la organización, o si los activos están expuestos a riesgos altos, se debería realizar entonces una segunda iteración, la evaluación de riesgo detallada, para ese activo de información particular (o parte del mismo).

Una regla general para aplicar: si la falta de seguridad de la información puede resultar en consecuencias adversas significantes para la organización, sus procesos o activos, entonces una segunda iteración de evaluación de riesgos, en un nivel más detallado, es necesaria para identificar riesgos potenciales.

E.2 Evaluación del riesgo de seguridad de la información detallada

E.2.1 Generalidades

El proceso de evaluación del riesgo de seguridad de la información detallado involucra una profunda identificación y evaluación de los activos, la evaluación de las amenazas a los activos, y la evaluación de las vulnerabilidades. El resultado de estas actividades es luego utilizado para valorar los riesgos e identificar el tratamiento de los mismos.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

El paso detallado generalmente requiere tiempo considerable, esfuerzo y experiencia, y puede entonces ser lo más adecuado para los sistemas de información en alto riesgo.

La etapa final del análisis de riesgo detallado es la valoración general de riesgos, la cual es el foco de este anexo.

Consecuencias pueden ser evaluadas de varias formas, incluyendo uso cuantitativo, por ejemplo, monetario, y medidas cualitativas (las cuales pueden basarse en el uso de adjetivos como moderado y severo), o una combinación de ambos. Para evaluar la probabilidad de ocurrencia de una amenaza, el marco de tiempo en el cual el activo va a tener valor o necesidad de protección puede ser establecido. La probabilidad de ocurrencia de una amenaza específica está afectada por lo siguiente:

- lo atractivo del activo, o posible impacto aplicable cuando una amenaza humana deliberada está siendo considerada;
- lo fácil que la explotación de una vulnerabilidad de un activo se convierta en una ganancia, aplicable si una amenaza humana deliberado está siendo considerada;
- las capacidades técnicas del agente de la amenaza, aplicable a amenazas humanas deliberadas; y
- lo susceptible de la vulnerabilidad a ser explotada, aplicable a ambas, técnicas y no técnicas vulnerabilidades.

Varios métodos utilizan tablas, y combinan medidas subjetivas y empíricas. Es importante que la organización use un método con el cual se sienta confortable, en el cual la organización confíe, y que produzca resultados repetibles. Algunos ejemplos de técnicas basadas en tablas son dados a continuación.

El estándar IEC 31010 brinda guías adicionales sobre técnicas que pueden ser utilizadas para una evaluación detallada del riesgo de seguridad de la información.

Los siguientes ejemplos utilizan números para describir las valoraciones cualitativas. Los usuarios de estos métodos deberían ser conscientes que puede ser inválido realizar operaciones matemáticas adicionales utilizando los números que son resultados cualitativos producidos por los métodos de valoración cualitativa de riesgos.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

E.2.2 Ejemplo 1 Matriz con valores predefinidos

En las valoraciones de riesgo de este tipo, los activos físicos actuales o prepuestos son valuados en términos de costos de reemplazo o reconstrucción (es decir medidas cuantitativas). Estos costos son luego convertidos a la misma escala cuantitativa que fue utilizada para la información. Adicionalmente, si se demuestra que algún software de aplicación tiene requerimientos intrínsecos de confidencialidad o integridad (por ejemplo si el código fuente es por sí mismo comercialmente sensitivo), el mismo es evaluado en la misma forma que la información.

Los valores para la información son obtenidos por entrevistas con gerentes de negocio seleccionados (los "propietarios" de los datos) los cuales pueden hablar con propiedad acerca de los datos, para determinar el valor y la sensibilidad de la información que se encuentra, en efecto, en uso, o a ser almacenada, procesada o accedida. Las entrevistas facilitan la evaluación de la sensibilidad y valor de la información en términos del escenario de peor caso que puede ser razonablemente esperado que ocurra como consecuencia adversa al negocio resultado de la divulgación indebida, modificación no autorizada, no disponibilidad en períodos de tiempo variables, y la destrucción.

La evaluación es realizada utilizando guías de valuación I de información, las cuales cubren aspectos como:

- seguridad personal;
- información personal y privacidad;
- aplicación de la ley;
- intereses comerciales y económicos;
- pérdida financiera y perturbación de las actividades;
- orden público;
- política de negocio y operaciones;
- pérdida de la buena voluntad; y
- contrato o acuerda con un cliente.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

Las guías facilitan la identificación de los valores en una escala numérica, como la escala de 0 a 4 mostrada en el ejemplo de la matriz de abajo, por lo tanto, permite el reconocimiento de los valores cuantitativos cuando sea posible y lógico, y cualitativos cuando los cuantitativos no sean posibles, por ejemplo peligro para la vida humana.

La próxima actividad importante es completar un par de cuestionarios para cada tipo de amenaza, para cada grupo de activos a los cuales un tipo de amenaza se relaciona, permitir la evaluación de los niveles de amenaza (probabilidad de ocurrencia) y niveles de vulnerabilidades (facilidad de explotación por una amenaza que causa consecuencias adversas). La respuesta a cada pregunta atrae un resultado. Estos resultados son acumulados en una base de conocimiento y comparados con rangos. Esto identifica niveles de amenaza "en decir" una escala de alto a bajo y niveles de vulnerabilidad en forma similar, como se muestra en el ejemplo de la matriz de abajo, diferenciando entre los tipos de consecuencias pertinentes. se debería que la información para completar los cuestionarios sea obtenida mediante entrevistas con los técnicos adecuados, el personal y las personas residentes, inspecciones físicas en las ubicaciones y revisión de documentación.

El valor de los activos, y los niveles de amenaza y vulnerabilidades, pertinentes a cada tipo de consecuencia, son emparejados en una matriz como la mostrada abajo, para identificar para cada combinación la medida pertinente de riesgo en una escala de 0 a 8. Los valores son puestos en la matriz en forma estructurada. Un ejemplo es dado abajo:

Tabla E.1

	Probabilidad de Ocurrencia - Amenaza	**Bajo**			**Medio**			**Alto**		
	Facilidad de Explotación	**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
Valor del activo	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Para cada activo, las vulnerabilidades pertinentes y sus correspondientes amenazas son consideradas. Si hay una vulnerabilidad sin una amenaza correspondiente, o una amenaza sin una vulnerabilidad correspondiente, no hay presente ningún riesgo (pero se debería

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

tener cuidado en caso que esta situación cambie). Ahora la fila apropiada en la matriz es identificada por el valor del activo, y la columna apropiada es identificada por la probabilidad de ocurrencia de la amenaza y la facilidad de explotación. Por ejemplo, si el activo tiene valor 3, la amenaza es "alta" y la vulnerabilidad "baja", la medida de riesgo es 5. Asuma que un activo tiene un valor de 2, por ejemplo, para la modificación, el nivel de amenaza es "baja" y la facilidad de explotación es "alta", entonces la medida del riesgo es 4. El tamaño de la matriz, en términos del número de categorías de probabilidad de amenaza, categorías de facilidad de explotación y número de categorías de evaluación de un activo, puede ser ajustado a las necesidades de la organización. Columnas y filas adicionales harán necesarias medidas del riesgo adicionales. El valor de este enfoque está en el ranking del riesgo a ser tratados.

Una Matriz similar a la mostrada en la Tabla E2 resulta de la consideración de la probabilidad del escenario de un incidente, correspondiente al impacto estimado en el negocio. La probabilidad de un escenario de un incidente está dada por una amenaza que explota una vulnerabilidad con una cierta probabilidad. La Tabla vincula esta probabilidad frente al impacto de negocio relacionado con el escenario del incidente. El riesgo resultante es medido en una escala de 0 a 8 que puede ser evaluada con respecto al criterio de aceptación de riesgos. Esta escala del riesgo podría también ser representada con una simple clasificación general de riesgos, por ejemplo, tal como:

- Riesgo Bajo: 0-2;
- Riesgo Medio: 3-5; y
- Riesgo Alto: 6-8.

Tabla E2

	Probabilidad del escenario de incidencia	**Muy bajo (Muy improbable)**	**Bajo (Improbable)**	**Medio (Posible)**	**Alto (Probable)**	**Muy alto (Frecuente)**
Impacto en el negocio	Muy bajo	0	1	2	3	4
	Bajo	1	2	3	4	5
	Medio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muy alto	4	5	6	7	8

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

E.2.3 Ejemplo 2 Ranking de las Amenazas por Medidas de Riesgos

Una matriz o una tabla, como se muestra en la tabla E.3, puede ser utilizada para relacionar los factores de las consecuencias (valor del activo) y la probabilidad de ocurrencia de una amenaza (teniendo en cuenta aspectos de la vulnerabilidad). El primer paso es evaluar las consecuencias (valor del activo) mediante una escala predefinida, por ejemplo 1 a 5, para cada activo amenazado (columna 'b' en la tabla). El segundo paso es evaluar la probabilidad de ocurrencia de la amenaza en una escala predefinida, por ejemplo 1 a 5, para cada amenaza (columna 'c' en la tabla). El tercer paso es calcular la medida del riesgo multiplicando (b x c). Finalmente, las amenazas pueden ser ordenadas de acuerdo a la medida del riesgo asociada. Nótese que, en este ejemplo, 1 es tomado como la menor consecuencia y la probabilidad de ocurrencia más baja.

Tabla E.3

Descripción de la amenaza (a)	Valor de la consecuencia (activo) (b)	Probabilidad de la ocurrencia de la amenaza (c)	Medida de riesgos (d)	Rankin de amenaza (e)
Amenaza A	5	2	10	2
Amenaza B	2	4	8	3
Amenaza C	3	5	15	1
Amenaza D	1	3	3	5
Amenaza E	4	1	4	4
Amenaza F	2	4	8	3

Como se muestra arriba, este es un procedimiento que permite que diferentes amenazas con diferentes consecuencias y probabilidad de ocurrencia sean comparadas y ordenadas por prioridad, como se muestra aquí. En algunos casos será necesario asociar valores monetarios a las escalas empíricas aquí utilizadas.

E.2.4 Ejemplo 3 Evaluar un valor para la probabilidad y las posibles consecuencias de riesgos

En este ejemplo, se hace énfasis en las consecuencias de un incidente de seguridad de la información (escenarios del incidente) y en la determinación de los sistemas a los cuales se debería dar prioridad. Esto se hace mediante la evaluación de dos valores para cada activo y riesgo, cuya combinación determinará el puntaje para cada activo. Cuando todos los

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

puntajes de los activos del sistema están sumados, una medida del riesgo para aquel sistema es determinada.

Primero un valor es asignado a cada activo. Este valor se refiere a las potenciales consecuencias adversas que pueden surgir si el activo es amenazado. Para cada amenaza aplicable al activo, este valor de activo es asignado al activo.

Luego un valor de probabilidad es evaluado. Esto es evaluado combinando la probabilidad de ocurrencia de la amenaza y la facilidad de explotación de la vulnerabilidad, véase Tabla E.4 que expresa la probabilidad de un escenario de incidente.

Tabla E.4

Probabilidad de la Amenaza	**Bajo**			**Medio**			**Alto**		
Niveles de Vulnerabilidad	**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
Valor de la Probabilidad de un escenario de incidente	0	1	2	1	2	3	2	3	4

A continuación, un puntaje de activo / amenaza se asigna al encontrar la intersección del valor del activo con el valor de la probabilidad en la Tabla E.5. Los puntajes activos/amenaza son totalizados para producir el puntaje total del activo. Esta cifra puede ser utilizada para diferenciar los activos que forman parte de un sistema.

Tabla E.5

Valor del activo	**0**	**1**	**2**	**3**	**4**
Valor de la Probabilidad					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

El paso final es sumar todos los puntajes totales de los activos del sistema, produciendo una puntuación para el sistema. Esto puede ser utilizado para distinguir entre sistemas y para determinar a cuál protección de sistema se debería dar prioridad.

En los ejemplos siguientes todos los valores son elegidos en forma aleatoria.

Suponga que el sistema S tiene tres activo A1, A2 y A3. También suponga que hay dos amenazas T1 y T2 aplicables al sistema S. Sea el valor de A1 es 3, de modo similar el valor del activo A2 es 2 y el valor del activo A3 es 4.

Si para A1 y T1 la probabilidad de amenaza es baja y la facilidad de explotación de la vulnerabilidad es media, entonces el valor de la probabilidad es 1 (Véase Tabla E.4).

El puntaje activo / amenaza A1/T1 puede ser obtenido de la Tabla E.5 como la intersección del valor del activo 3 y la probabilidad valor 1, o sea 4. Asimismo, si para A1/T2 la probabilidad de amenaza es media y la facilidad de explotación de vulnerabilidad es alta, el puntaje de A1/T2 es 6.

Ahora el puntaje total del activo A1T puede ser calculado, y es 10. El resultado total es calculado para cada activo y amenaza aplicable. El puntaje total del sistema es calculado sumando A1T + A2T + A3T para dar ST.

Ahora los diferentes sistemas pueden ser comparados para establecer las prioridades y también diferentes activos dentro del sistema.

El ejemplo anterior se muestra en términos de sistemas de información, sin embargo, un enfoque similar puede ser aplicado a procesos de negocio.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

ANEXO F
(INFORMATIVO)

Restricciones para la modificación del riesgo

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Se debería considerar dentro de las restricciones para la reducción del riesgo las siguientes:

- Restricciones de tiempo:

  Pueden existir muchos tipos de restricciones de tiempo. Por ejemplo, los controles deberían implementarse dentro de un período de tiempo aceptable para la dirección de la organización. Otro tipo de restricción de tiempo es si un control puede ser implementado dentro del tiempo de vida de la información o del sistema. Un tercer tipo de restricción de tiempo puede ser el período de tiempo que la dirección de la organización decide que es un período aceptable para estar expuesto a un riesgo particular.

- Restricciones financieras:

  La implementación o el mantenimiento de controles no debería ser más costoso que el valor del riesgo a proteger por esos controles, excepto cuando sea obligatorio (por ejemplo, por la legislación). se debería hacer un esfuerzo para no exceder los presupuestos asignados y obtener ventajas financieras a través de la aplicación de estos controles. Sin embargo, en algunos casos puede no ser posible alcanzar la seguridad deseada y el nivel de aceptación del riesgo debido a restricciones presupuestales. La resolución de esta situación requiere de la decisión de la dirección de la organización.

  Se debería tener mucho cuidado si el presupuesto reduce el número o calidad de los controles a ser implementados ya que esto puede conducir a la retención implícita del riesgo mayores a los planificados. se debería que el presupuesto establecido para los controles sea utilizado cuidadosamente como factor limitante.

- Restricciones técnicas:

  Problemas técnicos, como la compatibilidad de programas o hardware, pueden ser evitados fácilmente si se toman en cuenta durante la selección de los controles. Además, la implementación retrospectiva de controles a un

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

proceso o sistema existente es con frecuencia obstaculizada por restricciones técnicas. Estas dificultades pueden mover el equilibrio de los controles hacia los aspectos de procedimiento y físicos de la seguridad. Podría ser necesario revisar el programa de seguridad de la información para alcanzar los objetivos de seguridad. Esto puede ocurrir cuando los controles no satisfacen los resultados esperados en cuanto a reducción del riesgo sin pérdidas de productividad.

- Restricciones operacionales:

  Las restricciones operacionales, tales como la necesidad de operar 24x7 aun con back-ups pueden resultar en una implementación costosa y compleja de los controles a menos que sean construidos dentro del diseño desde el inicio.

- Restricciones culturales:

  Las restricciones culturales para la selección de los controles pueden ser específicas de un país, sector, organización o incluso de un departamento dentro de una organización. No todos los controles pueden ser aplicados en todos los países. Por ejemplo, puede ser posible implementar la revisión de bolsos en algunas partes de Europa, pero no en otras partes de Medio Oriente. Los aspectos culturales no pueden ser ignorados porque muchos controles dependen del apoyo activo del personal. Si el personal no entiende la necesidad de un control o no lo encuentra culturalmente aceptable, el control se volverá inefectivo con el paso del tiempo.

- Restricciones éticas:

  Las restricciones éticas pueden tener implicaciones importantes sobre los controles tales como cambios en la ética basados en normas sociales. Esto puede evitar la implementación de controles tales como la revisión de e-mails en algunos países. La privacidad de la información también puede cambiar dependiendo de la ética de la región o del gobierno. Esto podría ser de mayor preocupación en algunos sectores de la industria que en otros, por ejemplo, gobierno y cuidados médicos.

- Restricciones ambientales:

  Los factores ambientales, tales como, disponibilidad de espacio, condiciones climáticas extremas, geografía urbana y natural del entorno pueden influir en la selección de controles. Por ejemplo, en algunos países puede ser necesaria la protección contra terremotos, pero no en otros.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

- Facilidad de uso:

  Una interfase tecnología-hombre pobre resultará en un error humano y puede hacer que un control se vuelva inútil. se debería que los controles sean seleccionados para proveer una facilidad de uso óptima al tiempo que permitan alcanzar un nivel aceptable de riesgo residual para el negocio. Los controles que son difíciles de utilizar impactarán en su efectividad, ya que los usuarios intentarán evadirlos o ignorarlos lo máximo posible. Los controles de acceso complejos dentro de una organización podrían alentar a los usuarios a encontrar métodos de acceso alternativos no autorizados.

- Restricciones de personal:

  La disponibilidad y el costo salarial de un conjunto de habilidades especializadas para implementar los controles, y la habilidad para mover el personal entre ubicaciones en condiciones operativas adversas, deberían ser considerados. La experiencia podría no estar disponible inmediatamente para implementar los controles planificados o la experiencia podría ser excesivamente costosa para la organización. Otros aspectos tales como la tendencia de algunos equipos de personal a discriminar a otros miembros del equipo que no son vigilados de forma segura pueden tener implicaciones mayores para las políticas y prácticas de seguridad. Asimismo, la necesidad de contratar a las personas adecuadas para el trabajo, y encontrar a las personas adecuadas, podría llevar a la contratación antes de que la investigación de la seguridad se complete. La práctica normal y más segura es requerir la investigación de antecedentes previo a la contratación.

- Restricciones de la integración de controles nuevos y ya existentes:

  La integración de nuevos controles en la infraestructura existente y las interdependencias entre los controles son con frecuencia vistas de forma superficial. Los nuevos controles podrían no ser fácilmente implementados si hay incongruencias o incompatibilidades con los controles existentes. Por ejemplo, un plan para el uso de dispositivos (tokens) biométricos para el control del acceso físico podría entrar en conflicto con un sistema existente basado en PIN-pad para el control del acceso. se debería que el costo de cambiar los controles existentes a los controles planificados incluya elementos a ser agregados a los costos globales de tratamiento de riesgos. Podría no ser posible la implementación de un control seleccionado debido a interferencias con los controles actuales.

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados

BIBLIOGRAFÍA

[1] ISO/IEC Guide 73, Risk management — Vocabulary

[2] ISO/IEC 16085, Systems and software engineering — Life cycle processes — Risk management

[3] ISO/IEC 27001[a], Information technology — Security techniques — Information security management systems — Requirements

[4] ISO/IEC 27002[b], Information technology — Security techniques — Code of practice for information security controls

[5] ISO 31000[c], Risk management — Principles and guidelines

[6] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

[7] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

[a] La NTP-ISO/IEC 27001:2014 es equivalente a la ISO/IEC 27001:2013 .
[b] La NTP-ISO/IEC 27002:2017 es equivalente a la ISO/IEC 27002:2013 .
[c] La NTP-ISO 31000 es equivalente a la ISO 31000 .

© ISO/IEC 2018 - © INACAL 2018 - Todos los derechos son reservados