PROYECTO DE
NORMA TÉCNICA COLOMBIANA NTC-ISO 27005 DE 174/08

PRÓLOGO

ISO (la Organización Internacional para la Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado de normalización mundial. Los organismos nacionales que son miembros de ISO o de IEC participan en el desarrollo de normas internacionales a través de los comités establecidos por la respectiva organización para tratar los campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en unión con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el comité ISO/IEC JTC 1.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las directrices de ISO/IEC.

La principal labor del comité técnico conjunto es preparar normas internacionales. Las versiones preliminares de las normas internacionales adoptadas por el comité técnico conjunto se dan a conocer a todos los organismos nacionales para la votación. La publicación como una Norma Internacional requiere la aprobación de 75 % mínimo de los organismos miembro que votan.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC no asumen responsabilidad por la identificación de cualquiera o todos los derechos de patente.

La norma ISO/IEC 27005 fue elaborada por el Comité Técnico Conjunto ISO/ IEC JTC 1, *Tecnología de la información*, Subcomité SC 27, *Técnicas de seguridad en la tecnología de la información.*

La primera edición de la norma ISO/IEC 27005 cancela y reemplaza a las normas ISO/IEC TR 13335-3:1998, e ISO/IEC TR 13335-4:2000, de las cuales constituye una revisión técnica.

PROYECTO DE
NORMA TÉCNICA COLOMBIANA NTC-ISO 27005 DE 174/08

CONTENIDO

Página

Página

FIGURAS

TABLA

Página

ANEXOS

INTRODUCCIÓN

Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. Corresponde a la organización definir su enfoque para la gestión del riesgo, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial. Se puede utilizar una variedad de metodologías existentes bajo la estructura descrita en esta norma para implementar los requisitos de un sistema de gestión de seguridad de la información.

Esta norma es pertinente para los directores y el personal involucrado en la gestión del riesgo en la seguridad de la información dentro de una organización y, cuando corresponda, para las partes externas que dan soporte a dichas actividades.

PROYECTO DE
NORMA TÉCNICA COLOMBIANA NTC-ISO 27005 DE 174/08

TECNOLOGÍA DE LA INFORMACIÓN.
TÉCNICAS DE SEGURIDAD.
GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma suministra directrices para la gestión del riesgo en la seguridad de la información.

Esta norma brinda soporte a los conceptos generales que se especifican en la norma ISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

El conocimiento de los conceptos, modelos, procesos y terminologías que se describen en la norma ISO/IEC 27001 y en ISO/IEC 27002 es importante para la total comprensión de esta norma.

Esta norma se aplica a todos los tipos de organizaciones (por ejemplo empresas comerciales, agencias del gobierno, organizaciones sin ánimo de lucro) que pretenden gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos de referencia son indispensables para la aplicación de esta norma. Para referencias con fecha, únicamente se aplica la edición citada. Para referencias sin fecha, se aplica en la edición más reciente del documento mencionado (incluyendo todas las enmiendas).

ISO/IEC 27001:2005, *Information Technology. Security Techniques. Information Security Management Systems. Requirements.*

ISO/IEC 27002:2005, *Information Technology. Security Techniques. Code of Practice for Information Security Management.*

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento, se aplican los términos y definiciones de las normas ISO/IEC 27001 e ISO/IEC 27002 y las siguientes:

3.1 Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

3.2 Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

NOTA Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.

3.3 Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

[ISO/IEC Guía 73:2002]

3.4 Comunicación del riesgo. Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.

[ISO/IEC Guía 73:2002]

3.5 Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

[ISO/IEC Guía 73:2002]

NOTA 1 En el contexto de esta norma, el término "actividad" se utiliza en lugar del término "proceso" para la estimación del riesgo.

NOTA 2 En el contexto de esta norma, el término "posibilidad" se utiliza en lugar del término "probabilidad" para la estimación del riesgo.

3.6 Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

[ISO/IEC Guía 73:2002]

NOTA En el contexto de esta norma, el término "actividad" se utiliza en lugar del término "proceso" para la identificación del riesgo.

3.7 Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

[ISO/IEC Guía 73:2002]

NOTA En el contexto de esta norma, el término "posibilidad" se utiliza en lugar del término "probabilidad" para la reducción del riesgo.

3.8 Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

[ISO/IEC Guía 73:2002]

NOTA En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la retención del riesgo.

3.9 Transferencia del riesgo. Compartir con otra de las partes la pérdida o la ganancia de un riesgo.
[ISO/IEC Guía 73:2002]

NOTA En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la transferencia del riesgo.

4. ESTRUCTURA DE ESTA NORMA

Esta norma contiene la descripción de los procesos para la gestión del riesgo en la seguridad de la información y sus actividades

La información general se proporciona en el numeral 5.

En el numeral 6 se suministra una visión general de los procesos de gestión del riesgo en la seguridad de la información.

Todas las actividades para la gestión del riesgo en la seguridad en la información se presentan en el numeral 6 y se describen posteriormente en los siguientes numerales:

- establecimiento del contexto, en el numeral 7;
- evaluación del riesgo, en el numeral 8;
- tratamiento del riesgo, en el numeral 9;
- aceptación del riesgo, en el numeral 10;
- comunicación del riesgo, en el numeral 11;
- monitoreo y revisión del riesgo, en el numeral 12.

En los anexos se presenta la información adicional para las actividades de la gestión del riesgo en la seguridad de la información. El establecimiento del contexto está sustentado por el Anexo A (que define el alcance y los límites del proceso de gestión del riesgo en la seguridad de la información). La identificación y evaluación de los activos y las evaluaciones del impacto se discuten en el Anexo B (ejemplos para activos), Anexo C (ejemplos de amenazas comunes) y Anexo D (ejemplos de vulnerabilidades comunes).
Los ejemplos de los enfoques para la evaluación del riesgo en la seguridad de la información se presentan en el Anexo E.

En el Anexo F se presentan las restricciones para la reducción del riesgo.

Todas las actividades para la gestión del riesgo que se presentan en los numerales 7 al 12 están estructuradas de la siguiente manera:

Entrada: identifica toda la información que se requiere para realizar la actividad.

Acciones: describe la actividad.

Guía de implementación: proporciona guías para llevar a cabo la acción. Algunas de ellas pueden no ser adecuadas en todos los casos y por ende otras formas de ejecutar la acción pueden ser más adecuadas.

Salida: identifica toda la información derivada después de realizar la actividad.

5. INFORMACIÓN GENERAL

Es necesario un enfoque sistemático para la gestión del riesgo en la seguridad de la información para identificar las necesidades de la organización con respecto a los requisitos de seguridad de la información y para crear un sistema de gestión de la seguridad de la información (SGSI) eficaz. Este enfoque debería ser adecuado para el entorno de la organización y, en particular, debería cumplir los lineamientos de toda la gestión del riesgo en la empresa. Los esfuerzos de seguridad deberían abordar los riesgos de una manera eficaz y oportuna donde y cuando sean necesarios. La gestión del riesgo en la seguridad de la información debería ser una parte integral de todas las actividades de gestión de seguridad de la información y se deberían aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.

La gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable.

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

- la identificación de los riesgos;
- La evaluación de los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia;
- La comunicación y entendimiento de la probabilidad y las consecuencias de estos riesgos ;
- El establecimiento del orden de prioridad para el tratamiento de los riesgos;
- La priorización de las acciones para reducir la ocurrencia de los riesgos;
- La participación de los interesados cuando se toman las decisiones sobre gestión del riesgo y mantenerlos informados sobre el estado de la gestión del riesgo;
- La eficacia del monitoreo del tratamiento del riesgo;
- El monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos;

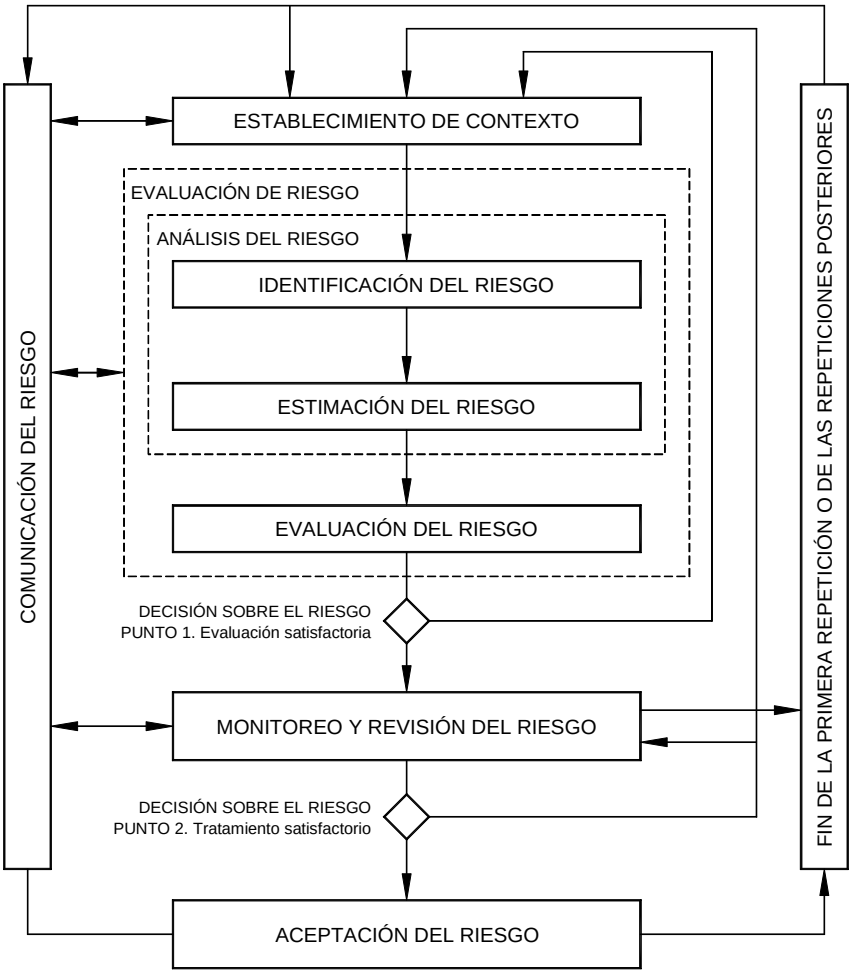
- La captura de información para mejorar el enfoque de la gestión de riesgos;

- La educación de los directores y del personal acerca de los riesgos y las acciones que se toman para mitigarlos.

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

6. VISIÓN GENERAL DEL PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

El proceso de gestión del riesgo en la seguridad de la información consta del establecimiento del contexto (véase el numeral 7), evaluación del riesgo (véase el numeral 8), tratamiento del riesgo (véase el numeral 9), aceptación del riesgo (véase el numeral 10), comunicación del riesgo (véase el numeral 11) y monitoreo y revisión del riesgo (véase el numeral 12).



Fin de la primera iteración o de las posteriores

Figura 1. Proceso de gestión del riesgo en la seguridad de la información

Así como lo ilustra la Figura 1, el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o de tratamiento del riesgo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos altos se valoren de manera correcta.

El contexto se establece primero. Luego se realiza una valoración del riesgo. Si ésta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos hasta un nivel aceptable, entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado (por ejemplo, los

criterios de evaluación del riesgo, los criterios para aceptar el riesgo o los criterios de impacto), posiblemente en partes limitadas del alcance total (véase la Figura 1, Decisión sobre el riesgo-punto 1).

La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual. En esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo criterios para valoración del riesgo, de aceptación o de impacto del riesgo), seguida del tratamiento del riesgo (véase la Figura 1, Decisión sobre el riesgo-punto 2).

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

Durante todo el proceso de gestión del riesgo en la seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los directores y al personal operativo correspondiente. Incluso antes del tratamiento de los riesgos, la información acerca de los riesgos identificados puede ser muy valiosa para la gestión de incidentes y puede ayudar a reducir el daño potencial. La toma de conciencia por parte de los directores y el personal acerca de los riesgos, la naturaleza de los controles establecidos para mitigar los riesgos y las áreas de interés para la organización facilitan el tratamiento de los incidentes y los eventos inesperados de una manera más eficaz. Se recomienda documentar los resultados detallados en cada actividad del proceso de gestión del riesgo en la seguridad de la información y de los dos puntos de decisión sobre el riesgo.

La norma ISO/IEC 27001 especifica que los controles implementados dentro del alcance, los límites y el contexto de SGSI se deben basar en el riesgo. La aplicación de un proceso de gestión del riesgo en la seguridad de la información puede satisfacer este requisito. Existen muchos enfoques mediante los cuales se puede implementar exitosamente el proceso en una organización. La organización debería utilizar cualquier enfoque que se ajuste mejor a sus circunstancias para cada aplicación específica del proceso.

En un SGSI, el establecimiento del contexto, la valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo son parte de la fase de "planificar". En la fase de "hacer" del SGSI, se implementan las acciones y los controles que son necesarios para reducir el riesgo hasta un nivel aceptable, de acuerdo con el plan de tratamiento del riesgo. En la fase de "verificar" del SGSI, los directores determinarán la necesidad de revisiones de las valoraciones y del tratamiento del riesgo a la luz de los incidentes y los cambios en las circunstancias. En la fase de "actuar", se llevan a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del SGSI:

Tabla 1. Alineamiento del SGSI y el proceso de Gestión del Riesgo en la Seguridad de la Información

Proceso de SGSI	Proceso de gestión del riesgo en la seguridad de la información

Planificar	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continuos de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

7. ESTABLECIMIENTO DEL CONTEXTO

7.1 CONSIDERACIONES GENERALES

Entrada: toda la información acerca de la organización que es pertinente para establecer el contexto de la gestión del riesgo en la seguridad de la información.

Acción: se debería establecer el contexto para la gestión del riesgo en la seguridad de la información, lo cual implica establecer los criterios básicos que son necesarios para la gestión del riesgo de la seguridad de la información (véase el numeral 7.2), definir el alcance y los límites (véase el numeral 7.3) y establecer una organización adecuada que opere la gestión del riesgo la seguridad de la información (véase el numeral 7.4).

Guía para la implementación:

Es esencial determinar el propósito de la gestión del riesgo en la seguridad de la información ya que esto afecta al proceso total y, en particular, al establecimiento del contexto. Este propósito puede ser:

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

La guía de implementación para los elementos del establecimiento del contexto que son necesarios para dar soporte a un SGSI se discute posteriormente en los numerales 7.2, 7.3 y 7.4.

NOTA La norma ISO/IEC 27001 no utiliza el término "contexto". Sin embargo, todo el numeral 7 de esta norma se relaciona con los requisitos de "definir el alcance y los límites del SGSI [(véase el numeral 4.2.1 a)], "definir la política de un SGSI" [(véase el numeral 4.2.1 b)] y "definir el enfoque para la evaluación del riesgo" [(véase el numeral 4.2.1 c)] que se especifican en la norma ISO/IEC 27001.

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

7.2 CRITERIOS BÁSICOS

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

Es aconsejable seleccionar o desarrollar un enfoque adecuado para la gestión del riesgo que aborde los criterios básicos tales como: criterios de evaluación del riesgo, criterios de impacto, criterios de aceptación del riesgo.

Además, la organización debería evaluar si los recursos necesarios están o no disponibles para:

- realizar la valoración del riesgo y establecer un plan de tratamiento para el riesgo;
- definir e implementar las políticas y los procedimientos, que incluyan la implementación de los controles seleccionados;
- monitorear los controles ;
- monitorear los procesos de gestión del riesgo en la seguridad de la información.

NOTA Véase también la norma ISO/IEC 27001 (numeral 5.2.1) con relación a la provisión de los recursos para la implementación y el funcionamiento de un SGSI.

Criterios de evaluación del riesgo

Se recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización, teniendo en cuenta los siguientes aspectos:

- el valor estratégico del proceso de información del negocio;
- la criticidad de los activos de información involucrados;
- los requisitos legales y reglamentarios, así como las obligaciones contractuales;
- la importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

De igual modo, los criterios de evaluación del riesgo se pueden utilizar para especificar las prioridades para el tratamiento del riesgo.

Criterios de impacto

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- nivel de clasificación de los activos de información impactados;
- brechas en la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad);
- operaciones deterioradas (partes internas o terceras partes);
- pérdida del negocio y del valor financiero;
- alteración de planes y fechas límites;
- daños para la reputación;
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

NOTA Véase también la norma ISO/IEC 27001 [numeral 4.2.1 d) 4] con respecto a la identificación de los criterios del impacto para las pérdidas de confidencialidad, integridad y disponibilidad.

Criterios de la aceptación del riesgo

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas.

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar los siguientes aspectos:

- los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas;
- los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado;
- los diferentes criterios de aceptación del riesgo se pueden aplicar a diferentes clases de riesgos, por ejemplo los riesgos que podrían resultar en incumplimiento con reglamentos o leyes, podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos, si esto se especifica como un requisito contractual;
- los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo, por ejemplo el riesgo puede estar asociado con una

actividad temporal o de corto plazo. Los criterios de aceptación del riesgo se deberían establecer considerando los siguientes elementos:

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

NOTA Los criterios de aceptación del riesgo corresponden a "los criterios para aceptar riesgos e identificar el nivel aceptable del riesgo" que se especifican en la norma ISO/IEC 27001, numeral 4.2.1 c) 2).

Información adicional se puede obtener en el Anexo A.

7.3 EL ALCANCE Y LOS LÍMITES

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

Es necesario definir el alcance del proceso de gestión del riesgo en la seguridad de la información, con el fin de garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo. Además, es necesario identificar los límites (véase también la norma ISO/IEC 27001, numeral 4.2.1 a) para abordar aquellos riesgos que se pueden presentar al establecer estos límites.

Se debería recolectar información acerca de la organización para determinar el ambiente en que ella funciona y establecer la pertinencia de la información para el proceso de gestión del riesgo en la seguridad de la información.

Al definir el alcance y los límites, la organización debería considerar la siguiente información:

- los objetivos estratégicos de negocio, políticas y estrategias de la organización;
- procesos del negocio;
- las funciones y estructura de la organización;
- los requisitos legales, reglamentarios y contractuales aplicables a la organización;
- la política de seguridad de la información de la organización;
- el enfoque global de la organización hacia la gestión del riesgo;

- activos de información;
- ubicación de la organización y sus características geográficas;
- restricciones que afectan a la organización;
- expectativas de las partes interesadas;
- entorno sociocultural;
- interfaces (Ejemplo: intercambio de información con el entorno).

Además, la organización debería suministrar la justificación para cualquier exclusión de este alcance.

Los ejemplos del alcance de la gestión del riesgo pueden ser una aplicación de tecnología de la información, infraestructura de tecnología de la información, un proceso del negocio o una parte definida de una organización.

NOTA El alcance y los límites de la gestión del riesgo en la seguridad de la información se relacionan con el alcance y los límites del SGSI que se exigen en la norma NTC-ISO/IEC 27001, 4.2.1 a).

Información adicional se puede obtener en el Anexo A.

7.4 ORGANIZACIÓN PARA LA GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Se recomienda establecer y mantener la organización y las responsabilidades en el proceso de gestión del riesgo y la seguridad de la información. Las siguientes son las principales funciones y responsabilidades en esta organización:

- Desarrollar el proceso de gestión del riesgo en la seguridad de la información que sea adecuado para la organización.
- Identificar y analizar las partes interesadas.
- Definir las funciones y las responsabilidades de todas las partes, tanto internas como externas, de la organización.
- Establecer las relaciones necesarias entre la organización y las partes interesadas, así como las interfaces con las funciones de la gestión del riesgo de alto nivel de la organización (por ejemplo, gestión del riesgo operativo), y las interfaces con otros proyectos o actividades relevantes.
- Definir las rutas para escalar decisiones.
- Especificar los registros que se deben conservar.

Esta organización para la gestión del riesgo, debería ser aprobada por los directores correspondientes de la entidad.

NOTA La norma NTC-ISO/IEC 27001 exige la determinación y el suministro de los recursos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI [(5.2.1 a)]. La organización de las operaciones de la gestión del riesgo se puede considerar como uno de los recursos exigidos por la norma NTC- ISO/IEC 27001.

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

8.1 DESCRIPCIÓN GENERAL DE LA VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

NOTA La actividad de valoración del riesgo esta referenciada como proceso en la norma ISO/IEC 27001.

Entrada: Criterios básicos, el alcance y los límites, y la organización establecida para el proceso de la gestión del riesgo en la seguridad de la información.

Acción: Los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la organización.

Guía para la implementación:

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los directores priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos.

La valoración del riesgo consta de las siguientes actividades:

- Análisis del riesgo (véase el numeral 8.2) el cual consiste en:
  - Identificación del riesgo (véase el numeral 8.2.1).
  - Estimación del riesgo (véase el numeral 8.2.2).
- Evaluación del riesgo (véase el numeral 8.3).

La valoración del riesgo determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables que existen (o que 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 clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido.

Con frecuencia, la valoración del riesgo se lleva a cabo en dos (o más) iteraciones. En primer lugar, se realiza una valoración general para identificar riesgos potencialmente altos que ameriten posterior valoración. La siguiente iteración puede implicar una consideración adicional en profundidad de los riesgos potencialmente altos revelados en la iteración inicial. Cuando estas actividades suministran información que no es suficiente para evaluar el riesgo, entonces se realiza un análisis más detallado, probablemente en partes del alcance total y, tal vez, utilizando un método diferente.

Depende de la organización seleccionar su propio enfoque para la valoración del riesgo con base en los objetivos y la meta de esta valoración.

En el Anexo E se puede encontrar la discusión sobre los enfoques para la valoración del riesgo en la seguridad de la información.

Salida: Una lista de los riesgos valorados, con prioridad de acuerdo con los criterios de evaluación del riesgo.

8.2 ANÁLISIS DEL RIESGO

8.2.1 Identificación del riesgo

8.2.1.1 Introducción a la identificación del riesgo

El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Los pasos que se describen en los siguientes numerales de la sección 8.2.1 deberían recolectar datos de entrada para la actividad de estimación del riesgo.

NOTA Las actividades que se describen en los siguientes numerales se pueden llevar a cabo en un orden diferente, dependiendo de la metodología que se aplique.

8.2.1.2 Identificación de los activos

Entrada: Alcance y límites para la valoración del riesgo que se va a realizar, lista de los componentes con sus propietarios, ubicación, funciones, etc.

Acción: Se deberían identificar los activos dentro del alcance establecido (se relaciona con la norma NTC-ISO/IEC 27001, numeral 4.2.1 d) 1)).

Guía para la implementación:

Un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software.

La identificación de los activos se debería llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo. El nivel de detalle utilizado en la identificación de los activos tendrá influencia en la cantidad total de información recolectada durante la valoración del riesgo. Este nivel se puede mejorar en iteraciones posteriores de la valoración del riesgo.

Se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización (véase el numeral 8.2.2.2 con relación a la valoración del activo).

El límite de la revisión es el perímetro definido de los activos de la organización que debe ser gestionado por parte del proceso de gestión del riesgo en la seguridad de la información.

Mayor información sobre la identificación y la valoración de los activos con relación a la seguridad de la información se puede obtener en el Anexo B.

Salida: una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia.

8.2.1.3 Identificación de las amenazas

Entrada: información sobre las amenazas obtenida de los propietarios de los activos, de los usuarios, de la revisión de incidentes, y de otras fuentes, incluidos los catálogos de amenazas externas.

Acción: se deberían identificar las amenazas y sus orígenes (se relaciona con la norma ISO/IEC 27001, numeral 4.2.1 d) 2)).

Guía para la implementación:

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deberían identificar genéricamente y por tipo (por ejemplo, acciones no autorizadas, daño físico, fallas técnicas) y, cuando sea adecuado, las amenazas individuales dentro de la clase genérica identificada. Esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas, pero teniendo en cuenta que el volumen de trabajo requerido es limitado.

Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

La entrada para la identificación de las amenazas y la estimación de la probabilidad de ocurrencia (véase el numeral 8.2.2.3) se puede obtener de los propietarios o los usuarios del activo, del personal de recursos humanos, del administrador de las instalaciones y de especialistas en seguridad de la información, expertos en seguridad física, área jurídica y otras organizaciones que incluyen organismos legales, bien sea autoridades, compañías de seguros y autoridades del gobierno nacional. Los aspectos ambientales y culturales se deben tener en cuenta cuando se consideran las amenazas.

La experiencia interna obtenida de los incidentes y las valoraciones anteriores de las amenazas, se deberían tomar en consideración en la valoración actual. Podría ser valioso consultar otros catálogos de amenazas (pueden ser específicas para una organización o un negocio) para completar la lista de amenazas genéricas, cuando sea pertinente. Los catálogos y las estadísticas sobre las amenazas están disponibles en organismos industriales, del gobierno nacional, organizaciones legales, compañías de seguros, etc.

Cuando se utilizan catálogos de amenazas o los resultados de valoraciones anteriores de las amenazas, es conveniente ser consciente de que existe un cambio continuo de las amenazas importantes, en especial si cambia el ambiente del negocio o los sistemas de información.

Mayor información sobre los tipos de amenazas puede encontrar en el Anexo C.

Salida: una lista de las amenazas con la identificación del tipo y el origen de la amenaza.

8.2.1.4 Identificación de los controles existentes

Entrada: documentación de los controles, planes para la implementación del tratamiento del riesgo.

Acción: se deberían identificar los controles existentes y los planificados.

Guía para la implementación:

Se debería realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo en la duplicación de los controles. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente - una referencia a los reportes de auditoría del SGSI ya existente debería limitar el tiempo que tarda esta labor. Si el control no funciona como se espera, puede causar vulnerabilidades. Es recomendable tomar en consideración la situación en la que el control seleccionado (o la estrategia) falla en su funcionamiento y, por lo tanto, se requieren controles complementarios para tratar de manera eficaz el riesgo identificado. En un SGSI, de acuerdo con ISO/IEC 27001, se tiene como soporte la revisión de la eficacia del control. Una forma de estimar el efecto del control es ver la manera en que reduce la probabilidad de ocurrencia de la amenaza y la facilidad de explotar la vulnerabilidad, o el impacto del incidente. Las revisiones por parte de la dirección y los reportes de auditoría también suministran información acerca de la eficacia de los controles existentes.

Los controles que se planifican para implementar de acuerdo con los planes de implementación del tratamiento del riesgo, se deberían considerar en la misma forma que aquellos ya implementados.

Un control existente o planificado se podría identificar como ineficaz, insuficiente o injustificado. Si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar, reemplazar por otro más adecuado o si debería permanecer, por ejemplo, por razones de costos.

Para la identificación de los controles existentes o planificados, las siguientes actividades pueden ser útiles:

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

- verificación con las personas responsables de la seguridad de la información (por ejemplo, el funcionario a cargo de la seguridad de la información y el funcionario a cargo de la seguridad del sistema de información, el administrador de la instalación o el director de operaciones) y los usuarios, en cuanto a qué controles están realmente implementados para el proceso de información o el sistema de información que se considera;

- efectuar una revisión en el sitio de los controles físicos, comparando aquellos implementados con la lista de los controles que deberían estar, y verificando aquellos implementados con respecto a si funcionan correctamente y de manera eficaz, o;

- revisión de los resultados de las auditorías internas.

Salida: una lista de todos los controles existentes y planificados, su estado de implementación y utilización.

8.2.1.5 Identificación de las vulnerabilidades

Entrada: lista de las amenazas conocidas, lista de los activos y los controles existentes.

Acción: se deberían identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o la organización (se relaciona con ISO/IEC 27001, numeral 4.2.1 d) 3)).

Guía para la implementación:

Se pueden identificar vulnerabilidades en las siguientes áreas:

- organización;
- procesos y procedimientos;
- rutinas de gestión;
- personal;
- ambiente físico;
- configuración del sistema de información;
- hardware, software o equipo de comunicaciones;
- dependencia de partes externas.

La sola presencia de una vulnerabilidad no causa daño por si misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el cual funciona. Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar en un riesgo.

Las vulnerabilidades pueden estar relacionadas con las propiedades de los activos que se pueden usar de una manera, o para un propósito, diferente del previsto cuando se adquirió o se elaboró el activo. Las vulnerabilidades que se originan desde fuentes diferentes se deben considerar, por ejemplo, aquellas intrínsecas o extrínsecas al activo.

Ejemplos de vulnerabilidades y métodos para la valoración de la vulnerabilidad se pueden encontrar en el Anexo D.

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

8.2.1.6 Identificación de las consecuencias

Entrada: una lista de los activos y una lista de los procesos del negocio, una lista de las amenazas y las vulnerabilidades, cuando corresponda, con respecto a los activos y su pertinencia.

Acción: se deberían identificar las consecuencias que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad de los activos (véase la norma ISO/IEC 27001, 4.2.1 d) 4)).

Guía para la implementación:

Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, etc.

Esta actividad identifica los daños o las consecuencias para la organización que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades en un incidente de seguridad de la información (véase la norma ISO/IEC 27002, sección 13). El impacto de los escenarios de incidente se determina tomando en consideración los criterios del impacto que se definen durante la actividad de establecimiento del contexto. Puede afectar a uno o más activos o a una parte de un activo. De este modo, los activos pueden tener valores asignados tanto para su costo financiero como por las consecuencias en el negocio, si se deterioran o se ven comprometidos. Las consecuencias pueden ser de naturaleza temporal o permanente como es el caso de la destrucción de un activo.

NOTA La norma ISO/IEC 27001 describe la ocurrencia de escenarios de incidente como "fallas de la seguridad".

Las organizaciones deberían identificar las consecuencias operativas de los escenarios de incidentes en términos de (pero no limitarse a):

- tiempo de investigación y reparación;
- pérdida de tiempo (trabajo);
- pérdida de oportunidad;
- salud y seguridad;
- costo financiero de las habilidades específicas para reparar el daño;
- imagen, reputación y buen nombre.

Detalles sobre la valoración de las vulnerabilidades críticas se pueden encontrar en el literal B.3, Valoración del impacto.

Salida: una lista de los escenarios de incidente con sus consecuencias relacionadas con los activos y los procesos del negocio.

8.2.2 Estimación del riesgo

8.2.2.1 Metodologías para la estimación del riesgo

El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores que implicaron a la organización. Una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias. En la práctica, con frecuencia se utiliza la estimación cualitativa en primer lugar para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes. Posteriormente puede ser necesario realizar un análisis más específico o cuantitativo de los riesgos importantes dado que es, por lo general, menos complejo y menos costoso realizar un análisis cualitativo que uno cuantitativo.

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

A continuación se describen los detalles de las metodologías para la estimación:

a) Estimación cualitativa:

La estimación cualitativa utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales (por ejemplo, alta, intermedia y baja) y la probabilidad de que ocurran dichas consecuencias. Una ventaja de la estimación cualitativa es su facilidad de comprensión por parte de todo el personal pertinente, mientras que una desventaja es la dependencia en la selección subjetiva de la escala.

Estas escalas se pueden adaptar o ajustar para satisfacer las circunstancias y se pueden utilizar descripciones diferentes para riesgos diferentes. La estimación cualitativa se puede utilizar:

- como una actividad de tamizado inicial para identificar los riesgos que requieren un análisis más detallado;
- cuando este tipo de análisis es adecuado para tomar decisiones;
- cuando los datos numéricos o los recursos no son adecuados para una estimación cuantitativa.

El análisis cualitativo debería utilizar información con base en hechos y datos, cuando estén disponibles.

b) Estimación cuantitativa:

La estimación cuantitativa utiliza una escala con valores numéricos (a diferencia de las escalas descriptivas utilizadas en la estimación cualitativa) tanto para las consecuencias como para la probabilidad, utilizando datos provenientes de varias fuentes. La calidad del análisis depende de lo completos y exactos que sean los valores numéricos, y de la validez de los modelos utilizados. En la mayoría de los casos, la estimación cuantitativa utiliza datos históricos sobre los incidentes, dando como ventaja que ésta pueda relacionarse directamente con los objetivos de seguridad de la información y los intereses de la organización. Una desventaja es la falta de tales datos sobre riesgos nuevos o debilidades en la seguridad de la información. Una desventaja del enfoque cuantitativo se puede presentar cuando no se dispone de datos basados en los hechos que se puedan auditar, creando así una ilusión del valor y la exactitud de la valoración del riesgo.

La forma en la cual se expresan las consecuencias y la probabilidad, y las formas en las cuales se combinan para proveer el nivel del riesgo varían de acuerdo con el tipo de riesgo y el propósito para el cual se va a utilizar la salida de la valoración del riesgo. La incertidumbre y la variabilidad tanto de las consecuencias como de la probabilidad se deberían ser consideradas en el análisis y comunicarse de manera eficaz.

8.2.2.2 Evaluación de las consecuencias

Entrada: una lista de los escenarios de incidentes pertinentes , que incluya la identificación de las amenazas, las vulnerabilidades, los activos afectados, las consecuencias para los activos y los procesos del negocio.

Acción: se debería evaluar el impacto en el negocio de la organización que pueda resultar de incidentes posibles o reales en la seguridad de la información, teniendo en cuenta las consecuencias de una brecha en la seguridad de la información, por ejemplo la pérdida de confidencialidad, integridad o disponibilidad de los activos (se relaciona con ISO/IEC 27001, numeral 4.2.1 e) 1)).

Guías para la implementación:

Después de identificar todos los activos bajo revisión, se deberían tener en cuenta los valores asignados a estos activos en la evaluación de las consecuencias.

El valor del impacto del negocio se puede expresar de manera cualitativa y cuantitativa, pero cualquier método para asignar valor monetario en general puede suministrar más información para la toma de decisiones y, por tanto, facilitar un proceso más eficiente de toma de decisiones.

La valoración de activos empieza con la clasificación de los activos de acuerdo con su criticidad, en términos de la importancia de los activos para cumplir los objetivos de negocio de la organización. La valoración se determina entonces utilizando dos medidas:

- el valor de reemplazo del activo: el costo de la limpieza de recuperación y de reemplazo de la información (si es posible);

- las consecuencias para el negocio por la pérdida o compromiso de los activos, tales como consecuencias adversas potenciales para el negocio y/o consecuencias legales o reglamentarias por la divulgación, modificación, no disponibilidad y/o destrucción de la información, y otros activos de información.

Esta valoración se puede determinar a partir del análisis del impacto del negocio. El valor, determinado por las consecuencias para el negocio, es en general significativamente superior al simple costo del reemplazo, dependiendo de la importancia del activo para la organización en el cumplimiento de los objetivos del negocio

La valoración de activos es un factor clave en la evaluación del impacto de un escenario de incidente, porque el incidente puede afectar a más de un activo (por ejemplo activos independientes) o únicamente una parte de un activo. Diferentes amenazas y vulnerabilidades tendrán impactos diferentes en los activos, por ejemplo la pérdida de confidencialidad, integridad o disponibilidad. La evaluación de las consecuencias, por tanto, se relaciona con la valoración de activos con base en el análisis del impacto en el negocio.

Las consecuencias del impacto del negocio se pueden determinar mediante el modelado de los resultados de un evento o grupo de eventos, o mediante la extrapolación a partir de estudios experimentales o datos anteriores.

Las consecuencias se pueden expresar en términos de criterios monetarios, técnicos o del impacto humano, u otros criterios pertinentes para la organización. En algunos casos, se requiere más que un valor numérico para especificar las consecuencias para diferentes tiempos, lugares, grupos o situaciones.

Las consecuencias en el tiempo y las finanzas se deberían medir con el mismo enfoque utilizado para la probabilidad de amenaza y vulnerabilidad. Se debe mantener la consistencia en el enfoque cuantitativo o cualitativo.

Mayor información tanto de la valoración de activos como de la evaluación del impacto se puede obtener en el Anexo B.

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

8.2.2.3 Evaluación de la probabilidad de incidentes

Entrada: una lista de los escenarios de incidentes pertinentes, que incluya la identificación de las amenazas, los activos afectados, las vulnerabilidades explotadas y las consecuencias para los activos y los procesos del negocio. Además, listas de todos los controles existentes y planificados, su eficacia, implementación y estado de utilización.

Acción: se debería evaluar la probabilidad de los escenarios de incidente (se relaciona con ISO/IEC 27001, numeral 4.2.1 e) 2)).

Guías para la implementación:

Después de identificar los escenarios de incidentes, es necesario evaluar la probabilidad de cada escenario y el impacto de que ocurra, utilizando técnicas de estimación cualitativas o cuantitativas. Se deberían tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas, teniendo en cuenta:

- la experiencia y las estadísticas aplicables para la probabilidad de la amenaza;

- para fuentes de amenaza deliberada: la motivación y las capacidades, las cuales cambiarán con el tiempo, y los recursos disponibles para los posibles atacantes, así como la percepción de atracción y vulnerabilidad de los activos para un posible atacante;

- para fuentes de amenaza accidental: factores geográficos como proximidad a plantas químicas o de petróleo, la probabilidad de condiciones climáticas extremas, y factores que pudieran tener influencia en los errores humanos y el mal funcionamiento del equipo;

- vulnerabilidades, tanto individuales como en conjunto;

- controles existentes y qué tan eficazmente reducen las vulnerabilidades.

Por ejemplo, un sistema información puede tener una vulnerabilidad para las amenazas de enmascaramiento de la identidad del usuario y mala utilización de los recursos. La vulnerabilidad de enmascaramiento de la identidad del usuario puede ser alta debido a la falta de autentificación del usuario. Por otra parte, la probabilidad de mala utilización de los recursos puede ser baja, a pesar de la falta de autentificación del usuario, dado que las formas para el mal uso de los recursos son limitadas.

Dependiendo de la necesidad de exactitud, los activos se podrían agrupar o podría ser necesario dividir los activos en sus elementos y relacionar los escenarios con los elementos. Por ejemplo, a través de lugares geográficos, la naturaleza de las amenazas para los mismos tipos de activos puede cambiar, o puede variar la eficacia de los controles existentes.

Salida: probabilidad de los escenarios de incidente (cuantitativa o cualitativa).

8.2.2.4 Nivel de estimación del riesgo

Entrada: una lista de los escenarios de incidente con sus consecuencias relacionadas con los activos y los procesos del negocio, y su probabilidad (cuantitativa o cuantitativa).

Acción: se deberían estimar el nivel de riesgo para todos los escenarios de incidente pertinentes (se relaciona con ISO/IEC 27001, numeral 4.2.1 e) 4).

Guía para la implementación:

La estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. Estos valores pueden ser cuantitativos o cualitativos. La estimación del riesgo se basa en las consecuencias evaluadas y la probabilidad. Además, la estimación puede

considerar el beneficio de los costos, los intereses de las partes involucradas y otras variables, según correspondan para la evaluación 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 para la estimación del riesgo en la seguridad de la información se pueden encontrar en el Anexo E.

Salida: una lista de los riesgos con niveles de valor asignado.

8.3 EVALUACIÓN DEL RIESGO

Entrada: una lista de los riesgos con niveles de valor asignado y criterios para la evaluación del riesgo.

Acción: se deberían comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación (se relaciona con ISO/IEC 27001, numeral 4.2.1 e) 4).

Guía para la implementación:

La naturaleza de las decisiones pertinentes para la evaluación del riesgo y los criterios de evaluación del riesgo que se utilizarán para tomar dichas decisiones, deben haber sido determinados durante el establecimiento del contexto. Estas decisiones y el contexto se deberían revisar con mayor detalle en esta etapa cuando se sabe más acerca de los riesgos particulares identificados. Con el fin de evaluar los riesgos, las organizaciones deberían comparar los riesgos estimados (utilizando métodos o enfoques seleccionados, tal como se discute en el Anexo E) con los criterios de evaluación del riesgo que se definieron durante el establecimiento del contexto.

Los criterios de evaluación del riesgo utilizados para tomar decisiones deberían ser consistentes con el contexto definido para la gestión del riesgo en la seguridad de la información externa e interna y deberían tomar en consideración los objetivos de la organización, los puntos de vista de las partes interesadas, etc. Las decisiones, tal como se toman en la actividad de evaluación del riesgo, se basan principalmente en el nivel aceptable de riesgo. Sin embargo, también es recomendable considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo. La agrupación de múltiples riesgos bajos o medios puede dar como resultado riesgos globales mucho más altos y es necesario tratarlos según corresponda.

Las consideraciones deberían incluir:

- *propiedades de la seguridad de la información*: si un criterio no es pertinente para la organización (por ejemplo la pérdida de confidencialidad), entonces todos los riesgos que tienen impacto sobre este criterio pueden no ser pertinentes;

- *la importancia de los procesos del negocio o de la actividad sustentada por un activo particular o un conjunto de activos*: si se determina que el proceso tiene importancia baja, los riesgos asociados con él deberían tener una consideración más baja que los riesgos que tienen impacto en procesos o actividades más importantes.

La evaluación del riesgo utiliza la comprensión del riesgo que se obtiene mediante el análisis del riesgo para tomar decisiones sobre acciones futuras. Las decisiones deberían incluir:

- si se debería realizar una actividad;

- prioridades para el tratamiento de los riesgos considerando los valores estimados de ellos.

Salida: una lista de los riesgos con prioridad de acuerdo con los criterios de evaluación del riesgo, con relación a los escenarios de incidente que llevan a tales riesgos.

9. TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

9.1 DESCRIPCIÓN GENERAL DEL TRATAMIENTO DEL RIESGO

Entrada: una lista de los riesgos con prioridad de acuerdo con los criterios de evaluación del riesgo, con relación a los escenarios de incidente que llevan a tales riesgos.

Acción: se deberían seleccionar controles para reducir, retener, evitar o transferir los riesgos y se debería definir un plan para tratamiento del riesgo.

Guía para la implementación:

Existen cuatro opciones disponibles para el tratamiento del riesgo: reducción del riesgo (véase el numeral 9.2), retención del riesgo (véase el numeral 9.3), evitación del riesgo (véase el numeral 9.4) y transferencia del riesgo (véase el numeral 9.5).

NOTA La norma ISO/IEC 27001, 4.2.1 f) 2) utiliza el término "aceptación del riesgo" en lugar de "retención del riesgo".

La Figura 2 ilustra la actividad del tratamiento del riesgo dentro de los procesos de gestión del riesgo en la seguridad de la información, como se presenta en la Figura 1.

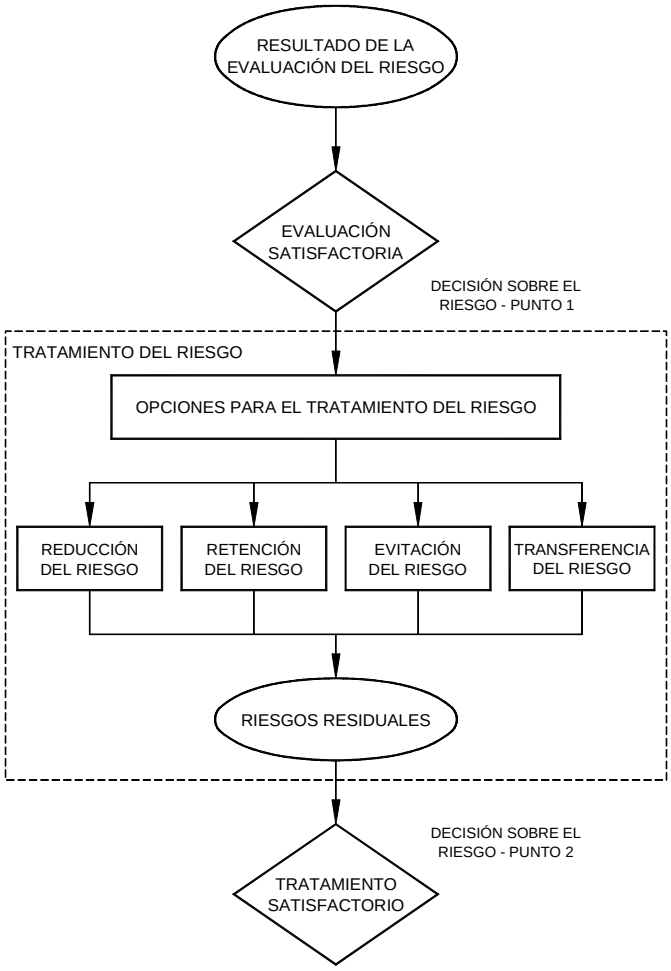


Figura 2. Actividad para el tratamiento del riesgo

Las opciones para el tratamiento del riesgo se deberían seleccionar con base en el resultado de la evaluación del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados como resultado de tales opciones.

Cuando se pueden obtener reducciones grandes en los riesgos con un costo relativamente bajo, se deberían implementar esas opciones. Las opciones adicionales para las mejoras pueden no ser económicas y es necesario estudiarlas para determinar si se justifican o no.

En general, las consecuencias adversas de los riesgos deberían ser tan bajas como sea razonablemente viable e independientemente de cualquier criterio absoluto. Los directores deberían tomar en consideración los riesgos raros pero graves. En tales casos, puede ser necesario implementar controles que nos son justificables en términos estrictamente económicos (por ejemplo, los controles para la continuidad del negocio considerados para cumplir riesgos altos específicos).

Las cuatro opciones para el tratamiento del riesgo no se excluyen mutuamente. En ocasiones, la organización se puede beneficiar significativamente de una combinación de opciones tales como la reducción de la probabilidad de los riesgos, reducción de sus consecuencias y transferencia o retención de los riesgos residuales.

Algunos tratamientos de los riesgos pueden tratar eficazmente más de un riesgo (por ejemplo, el entrenamiento y la toma de conciencia sobre la seguridad de la información). Conviene definir un plan para el tratamiento del riesgo que identifique con claridad el orden de prioridad en el cual se deberían implementar los tratamientos individuales, así como sus marcos temporales. Las prioridades se pueden establecer utilizando diversas técnicas, que incluyen clasificación del riesgo y análisis de costo-beneficio. Es responsabilidad de los directores de la organización decidir el equilibrio entre los costos de la implementación de los controles y la asignación de presupuesto.

La identificación de los controles existentes puede determinar que tales controles exceden las necesidades actuales, en términos de comparaciones de costo, incluyendo el mantenimiento. Si se considera la eliminación de controles redundantes o necesarios (especialmente si los controles tienen altos costos de mantenimiento), es conveniente tener en cuenta la seguridad de la información y los factores de costo. Dado que los controles pueden tener influencia entre sí, la eliminación de los controles redundantes podría reducir la seguridad global establecida. Además, puede ser más económico dejar los controles redundantes o innecesarios en su lugar antes que eliminarnos.

Las opciones para el tratamiento del riesgo se deberían considerar teniendo en cuenta:

- cómo perciben el riesgo las partes afectadas;

- la forma más adecuada de comunicación con dichas partes.

El establecimiento del contexto (véase el numeral 7.2 - Criterios de evaluación del riesgo) suministra información sobre los requisitos legales y reglamentarios que la organización debe cumplir. El riesgo para las organizaciones es la falla en el cumplimiento y se recomienda implementar opciones de tratamiento para limitar esta probabilidad. Todas las restricciones - organizativas, técnicas, estructurales, etc.- que se identifican durante la

actividad de establecimiento del contexto se deberían tomar en consideración durante el tratamiento del riesgo.

Una vez se ha definido el plan para el tratamiento del riesgo, es necesario determinar los riesgos residuales. Esto implica una actualización o repetición de la evaluación del riesgo, considerando los efectos esperados del tratamiento propuesto para tal riesgo. Si el riesgo residual aún no satisface los criterios de aceptación del riesgo de la organización, puede ser necesaria otra repetición del tratamiento del riesgo antes de proceder con la aceptación del riesgo. Mayor información se puede encontrar en ISO/IEC 27002, numeral 0.3.

Salida: plan para el tratamiento del riesgo y riesgos residuales sujetos a la decisión de aceptación de los directores de la organización.

9.2 REDUCCIÓN DEL RIESGO

Acción: el nivel del riesgo se debería reducir mediante la selección de controles, de manera tal que el riesgo residual se pueda revaluar como aceptable.

Guía para la implementación:

Se recomienda seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la evaluación y el tratamiento del riesgo. En esta selección se deberían tener en cuenta los criterios de aceptación del riesgo así como nuevos requisitos legales, reglamentarios y contractuales. En esta selección también se deberían considerar los costos y el marco temporal para la implementación de los controles, o los aspectos técnicos, ambientales y culturales. Con frecuencia es posible disminuir el costo total de la propiedad de un sistema con controles de seguridad de la información adecuadamente seleccionados.

En general, los controles pueden brindar uno o más de los siguientes tipos de protección: corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y concienciación. Durante la selección del control es importante ponderar el costo de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles en comparación con el valor de los activos que se protegen. Además, el retorno de la inversión en términos de reducción del riesgo y el potencial para explotar nuevas oportunidades de ejecución que brindan algunos controles también se deberían tomar en consideración. También conviene considerar las habilidades especializadas que pueden ser necesarias para definir e implementar nuevos controles o modificar los existentes.

La norma ISO/IEC 27002 proporciona información detallada sobre los controles.

Existen muchas restricciones que puede afectar la selección de los controles. Las restricciones técnicas tales como los requisitos de desempeño, el manejo (requisitos de soporte operativo) y los aspectos de compatibilidad pueden dificultar el uso de algunos controles o podrían inducir error humano bien sea anulando el control, dando una falsa sensación de seguridad o incluso aumentando el riesgo de modo que no haya control (por ejemplo exigiendo contraseñas complejas sin entrenamiento adecuado, haciendo que los usuarios escriban las contraseñas). Además, podría darse el caso de que un control

pueda afectar el desempeño. Los directores deberían intentar la identificación de una solución que satisfaga los requisitos de desempeño al tiempo que garantizan suficiente seguridad de la información. El resultado de este paso es una lista de los controles posibles, con sus costos, beneficios y prioridades de implementación.

Es conveniente considerar varias restricciones al seleccionar los controles y durante la implementación. Por lo común, se consideran los siguientes aspectos:

- restricciones de tiempo;
- restricciones financieras;
- restricciones técnicas;
- restricciones operativas;
- restricciones culturales;
- restricciones éticas;
- percepciones ambientales;
- restricciones legales;
- facilidad de utilización;
- restricciones personales.
- restricciones para la integración de controles nuevos y existentes.

En el Anexo F de puede encontrar mayor información sobre las restricciones para la reducción del riesgo.

9.3 RETENCIÓN DEL RIESGO

Acción: la decisión sobre la retención del riesgo sin acción posterior se debería tomar dependiendo de la evaluación del riesgo.

NOTA La normal ISO/IEC 27001, 4.2.1 f) 2), "aceptar los riesgos objetivamente y con conocimiento, siempre y cuando ellos satisfagan claramente las políticas de la organización y los criterios para la aceptación de los riesgos", describe la misma actividad.

Guía para la implementación:

Si el nivel del riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede retener.

9.4 EVITACIÓN DEL RIESGO

Acción: se debería evitar la actividad o la acción que da origen al riesgo particular.

Guía para la implementación:

Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad. Por ejemplo, para los riesgos causados por la naturaleza, puede ser una alternativa más eficaz en términos de costo, transferir físicamente las instalaciones de procesamiento de la información a un lugar donde no exista el riesgo o esté bajo control.

9.5 TRANSFERENCIA DEL RIESGO

Acción: el riesgo se debería transferir a otra de las partes que pueda manejar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo.

Guía para la implementación:

La transferencia del riesgo involucra una decisión para compartir algunos riesgos con las partes externas. La transferencia del riesgo puede crear riesgos nuevos o modificar los riesgos identificados existentes. Por lo tanto, puede ser necesario el tratamiento adicional para el riesgo.

La transferencia se puede hacer mediante un seguro que dará soporte a las consecuencias o mediante subcontratación de un asociado cuya función será monitorear el sistema de información y tomar acciones inmediatas para detener un ataque antes de que éste produzca un nivel definido de daño.

Conviene anotar que puede ser posible transferir la responsabilidad para la gestión del riesgo, pero normalmente no es posible transferir la responsabilidad de un impacto. Los clientes por lo general atribuirán un impacto adverso a fallas de la organización.

10. ACEPTACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Entrada: plan para el tratamiento del riesgo y evaluación del riesgo residual, sujetos a la decisión de aceptación de los directores de la organización.

Acción: se debería tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarla de manera formal (esto se relacionan con ISO/IEC 27001, párrafo 4.2.1 h)).

Guía para la implementación:

Los planes para el tratamiento del riesgo deberían describir la forma en que los riesgos evaluados se deben tratar, con el fin de satisfacer los criterios de aceptación del riesgo (véase numeral 7.2, Criterios de aceptación del riesgo). Es importante que los directores responsables revisen y aprueben los planes propuestos para el tratamiento del riesgo y los riesgos residuales resultantes, y que registren todas las condiciones asociadas a tal aprobación.

Los criterios de aceptación del riesgo pueden ser más complejos que sólo determinar si un riesgo residual está o no por encima o por debajo de un solo umbral.

En algunos casos, es posible que el nivel del riesgo residual no satisfaga los criterios de aceptación del riesgo porque los criterios que se aplican no toman en consideración las circunstancias prevalentes. Por ejemplo, se puede argumentar que es necesario aceptar los riesgos porque los activos físicos que los acompañan son muy atractivos o porque el costo de la reducción del riesgo es demasiado alto. Dicha circunstancia indica que los criterios de aceptación del riesgo no son adecuados y, si es posible, se deberían revisar. No obstante, no siempre es posible revisar los criterios de aceptación del riesgo de manera oportuna. En tales casos, quienes toman las decisiones pueden tener que aceptar riesgos que no satisfacen los criterios normales de aceptación. Si esto es necesario, quienes toman la decisión deberían comentar explícitamente los riesgos e incluir una justificación para la decisión de hacer caso omiso de los criterios normales de aceptación del riesgo.

Salida: una lista de los riesgos aceptados con la justificación para aquellos que no satisfacen los criterios normales de aceptación de riesgos de la organización.

11. COMUNICACIÓN DE LOS RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Entrada: toda la información sobre el riesgo obtenida a partir de las actividades de gestión del riesgo (véase la Figura 1).

Acción: la información acerca del riesgo se debería intercambiar y/o compartir entre la persona que toma la decisión y las otras partes involucradas.

Guía para la implementación:

La comunicación del riesgo es una actividad para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información acerca de los riesgos, entre quienes toman las decisiones y las otras partes involucradas. La información incluye, pero no se limita a la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos.

La comunicación eficaz entre las partes involucradas es importante dado que puede tener un impacto significativo en las decisiones que se deben tomar. La comunicación garantizará que aquellos responsables de la implementación de la gestión del riesgo y aquellos con derechos adquiridos comprenden las bases sobre las cuales toman las decisiones y el porqué se requieren acciones particulares. La comunicación es bidireccional.

Las percepciones del riesgo pueden variar debido a las diferencias en las estimaciones, los conceptos y las necesidades, los problemas y los intereses de las partes involucradas en cuanto se relacionan con el riesgo, o los aspectos bajo discusión. Es probable que las partes involucradas hagan juicios sobre la aceptabilidad del riesgo con base en su percepción de éste. Es particularmente importante garantizar que las percepciones que tienen las partes involucradas sobre el riesgo, así como sus percepciones de los beneficios se pueden identificar y documentar, y que las razones de base se comprendan y traten claramente.

La comunicación del riesgo se debería realizar con el fin de lograr lo siguiente:

- brindar seguridad del resultado de la gestión del riesgo de la organización;
- recolectar información sobre el riesgo;
- compartir los resultados de la evaluación del riesgo y presentar el plan para el tratamiento del riesgo;
- evitar o reducir tanto la ocurrencia como la consecuencia de las brechas en la seguridad de la información debidas a la falta de comprensión mutua entre quienes toman las decisiones y las partes involucradas;
- brindar soporte para la toma de decisiones;
- obtener conocimientos nuevos sobre la seguridad de la información;

- coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente;

- dar a quienes toman las decisiones y a las partes involucradas un sentido de responsabilidad acerca de los riesgos;

- Mejorar la concienciación.

Una organización debería desarrollar planes de comunicación del riesgo para las operaciones normales así como para las situaciones de emergencia. Por lo tanto, la actividad de comunicación del riesgo se debería realizar de manera continua.

La coordinación entre las personas principales que toman las decisiones y las partes involucradas se puede lograr mediante la formación de un comité en el cual pueda tener lugar el debate acerca de los riesgos, su prioridad, el tratamiento adecuado y la aceptación.

Es importante cooperar con las unidades correspondientes de relaciones públicas o comunicaciones dentro de la organización para coordinar todas las labores que se relacionan con la comunicación del riesgo. Esto es importante en el caso de acciones de comunicación de crisis, por ejemplo, en respuesta a incidentes particulares.

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

12. MONITOREO Y REVISIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

12.1 MONITOREO Y REVISIÓN DE LOS FACTORES DE RIESGO

Entrada: toda la información sobre el riesgo obtenida en las actividades de gestión del riesgo (véase la Figura 1).

Acción: los riesgos y sus factores (es decir, el valor de los activos, los impactos, las amenazas, las vulnerabilidades, la probabilidad de ocurrencia) se deberían monitorear y revisar con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana, y para mantener una visión general de la perspectiva completa del riesgo.

Guía para la implementación:

Los riesgos no son estáticos. Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación. Por ende, es necesario el monitoreo constante para detectar estos cambios. Esta actividad puede estar soportada por servicios externos que brinden información con respecto a nuevas amenazas o vulnerabilidades.

Las organizaciones deberían garantizar el monitoreo continuo de los siguientes aspectos:

- activos nuevos que se han incluido en el alcance de la gestión del riesgo;

- modificaciones necesarias de los valores de los activos, debido, por ejemplo, a cambios en los requisitos de negocios;

- amenazas nuevas que podrían estar activas tanto fuera como dentro de la organización y que no se han evaluado;

- probabilidad de que las vulnerabilidades nuevas o aumentadas puedan permitir que las amenazas exploten tales vulnerabilidades nuevas o con cambios;

- vulnerabilidades identificadas para determinar aquellas que se exponen a amenazas nuevas o que vuelven a emerger;

- el impacto aumentado o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo;

- incidentes de la seguridad de la información.

Las amenazas, vulnerabilidades o cambios nuevos en la probabilidad o las consecuencias pueden incrementar los riesgos evaluados previamente como riesgos bajos. En la revisión de los riesgos bajos y aceptados se debería considerar cada riesgo independientemente, y también todos estos riesgos como un conjunto, para evaluar su impacto acumulado potencial. Si los riesgos no están en la categoría de riesgo aceptable o bajo, se debería tratar utilizando una o más de las opciones que se consideran en el numeral 9.

Los factores que afectan a la probabilidad ya las consecuencias de las amenazas que se presentan podrían cambiar, como lo harían los factores que afectan a la idoneidad o el costo de las diversas opciones de tratamiento. Los cambios importantes que afectan a la organización debería ser la razón para una revisión más específica. Por lo tanto, las actividades de monitoreo del riesgo de deberían repetir con regularidad y las opciones seleccionadas para el tratamiento del riesgo se deberían revisar periódicamente.

El resultado de las actividades de monitoreo del riesgo puede ser la entrada para otras actividades de revisión del riesgo. La organización debería revisar todos los riesgos con regularidad, y cuando se presenten cambios importantes (de acuerdo con ISO/IEC 27001, numeral 4.2.3)).

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

12.2 MONITOREO, REVISIÓN Y MEJORA DE LA GESTIÓN DEL RIESGO

Entrada: toda la información sobre el riesgo obtenida en las actividades de gestión del riesgo (véase Figura 1).

Acción: el proceso de gestión del riesgo en la seguridad de la información se debería monitorear, revisar y mejorar continuamente, según sea necesario y adecuado.

Guía para la implementación:

El monitoreo y la revisión continuos son necesarios para garantizar que el contexto, el resultado de la evaluación del riesgo y el tratamiento del riesgo, así como los planes de gestión siguen siendo pertinentes y adecuados para las circunstancias.

La organización debería garantizar que el proceso de gestión del riesgo en la seguridad de la información y las actividades relacionadas aún son adecuadas en las circunstancias actuales y se cumplen. Todas las mejoras acordadas para el proceso o las acciones necesarias para mejorar la conformidad con el proceso se deberían notificar a los directores correspondientes para tener seguridad de que no se omite ni subestima ningún riesgo o elemento del riesgo, y que se toman las acciones necesarias y las decisiones para brindar una comprensión realista del riesgo y la capacidad para responder.

Además, la organización debería verificar con regularidad que los criterios utilizados para medir el riesgo y sus elementos aún son válidos y consistentes con los objetivos, las estrategias y las políticas del negocio, y que los cambios en el contexto del negocio se toman en consideración de manera adecuada durante el proceso de gestión del riesgo en la seguridad de la información. Esta actividad de monitoreo y revisión debería abordar los siguientes aspectos (pero no limitarse a ellos):

- contexto legal y ambiental;
- contexto de competición;
- enfoque para la evaluación del riesgo;
- categorías y valor de los activos;
- criterios del impacto;
- criterios de evaluación del riesgo;
- criterios de aceptación del riesgo;
- costo total de la propiedad;
- recursos necesarios.

La organización debería garantizar que los recursos para el tratamiento y la evaluación del riesgo están disponibles continuamente para revisar el riesgo, tratar las amenazas o vulnerabilidades nuevas o con cambios y asesorar a la dirección según corresponda.

El monitoreo de la gestión del riesgo puede dar como resultado una modificación o adición al enfoque, en la metodología o los instrumentos utilizados dependiendo de:

- cambios identificados;
- repetición de la evaluación del riesgo;
- metas del proceso de gestión del riesgo en la seguridad de la información (por ejemplo, continuidad del negocio, flexibilidad ante los incidentes, conformidad);

- objetivo del proceso de gestión del riesgo en la seguridad de la información (por ejemplo, organización, unidad de negocios, proceso de información, su implementación técnica, aplicación, conexión con Internet).

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

ANEXO A
(Informativo)

DEFINICIÓN DEL ALCANCE Y LOS LÍMITES DEL PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

A.1 ESTUDIO DE LA ORGANIZACIÓN

Estudio de la organización. El estudio de la organización convoca los elementos característicos que definen la identidad de una organización. Esto implica el propósito, el negocio, las misiones, los valores y las estrategias de esta organización. Estas características se deberían identificar junto con los elementos que contribuyen a su desarrollo (por ejemplo, la subcontratación).

La dificultad de esta actividad está en entender con exactitud la forma en que se estructura la organización. La identificación de su estructura real proporcionará la comprensión de la función y la importancia de cada división para alcanzar los objetivos de la organización.

Por ejemplo, el hecho de que el director de seguridad de la información se reporte ante la alta gerencia en lugar de hacerlo ante los directores de tecnología de la información puede indicar la participación de la alta gerencia en la seguridad de la información.

Propósito principal de la organización. El propósito principal de una organización se puede definir como la razón por la cual ella existe (su campo de actividad, su segmento del mercado, etc.).

Su negocio. El negocio de la organización, definido por las técnicas y el conocimiento de sus empleados, le permite alcanzar sus misiones. Es específico para el campo de actividad de la organización y, a menudo, define su cultura.

Su misión. La organización logra su propósito alcanzando su misión. Para identificar su misione, es recomendable identificar los servicios suministrados y/o los productos manufacturados con relación a los usuarios finales.

Sus valores. Los valores son los principios más importantes o el código de conducta bien definido que se aplica al ejercicio de un negocio. Puede involucrar al personal, las relaciones con agentes externos (clientes, etc.), la calidad de los productos suministrados o de los servicios prestados

Tome el ejemplo de una organización cuyo propósito es el servicio público, cuyo negocio es el transporte y cuyas misiones incluyen el transporte de niños hacia y desde 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 está bajo la autoridad de un director de división, responsable de las decisiones estratégicas, administrativas y operativas con respecto a su unidad;

- estructura funcional: la autoridad funcional se ejerce en los procedimientos, la naturaleza del trabajo y, algunas veces, las decisiones o la planificación (por ejemplo, producción, tecnología de información, recursos humanos, mercadeo, etc.).

Observaciones:

- una división dentro de una organización con estructura divisional puede estar organizada como una estructura funcional y viceversa;

- se puede decir que una organización tiene una estructura de matriz si tiene elementos de ambos tipos de estructura;

- en cualquier estructura organizacional se pueden diferenciar los siguientes niveles:

    - el nivel de toma de decisiones (definición de las orientaciones estratégicas);

    - el nivel de liderazgo (coordinación y gestión);

    - el nivel operativo (actividades de producción y soporte).

Cuadro de la organización. La estructura de la organización se representa de manera esquemática en un cuadro de la organización. Esta representación debería resaltar las líneas de reporte y delegación de autoridad, pero también debería incluir otras relaciones que, aún si no se basan en ninguna autoridad formal, son líneas de flujo de información.

Estrategia de la organización. Esto requiere de una expresión formal de los principios que guían a la organización. La estrategia de la organización determina la dirección y el desarrollo necesarios con el fin de obtener beneficios de los aspectos en juego y de los cambios importantes que se planifican.

A.2 LISTADO DE LAS RESTRICCIONES QUE AFECTAN A LA ORGANIZACIÓN

Es recomendable tomar en consideración todas las restricciones que afectan a la organización y que determinan su orientación en seguridad de la información. Los orígenes pueden estar dentro de la organización, en cuyo caso ésta tiene algún control sobre ellas, o fuera de la organización y por lo tanto, en general, no son negociables. Las restricciones de recursos (presupuesto, personal) y las restricciones de emergencias están entre las más importantes.

La organización determina sus objetivos (con respecto a su negocio, comportamiento, etc.), comprometiéndose con un camino determinado, posiblemente en un periodo largo de tiempo. Define en lo que se quiere convertir y los medios que necesitará para la implementación. Al especificar este camino, la organización tiene en cuenta los progresos en las técnicas, el conocimiento y experiencia, los deseos expresados de los usuarios, los clientes, etc. Este objetivo se puede expresar en forma de estrategias de desarrollo u operativas con la meta de, por ejemplo, disminuir los costos operativos, mejorar la calidad del servicio, etc.

Estos estrategias incluyen probablemente la información y el sistema información (SI), que facilita su aplicación. En consecuencia, las características relacionadas con identidad, misión y estrategias de la organización son elementos fundamentales en el análisis del problema dado que la brecha en un aspecto de seguridad de la información podría dar como resultado un replanteamiento de estos objetivos estratégicos. Además, es esencial que las propuestas para los requisitos de la seguridad de la información permanezcan consistentes con las reglas, los usos y los medios establecidos en la organización.

El listado de restricciones incluye las siguientes, pero no se limita a ellas:

Restricciones de naturaleza política

Estas restricciones pueden implicar a las administraciones del gobierno, instituciones públicas o, en términos más generales, a cualquier organización que deba aplicar decisiones del gobierno. Por lo común, son decisiones relacionadas con la orientación operativa o estratégica, tomadas por una división del gobierno o un organismo encargado de tomar decisiones, y se deberían aplicar.

Por ejemplo, la sistematización de facturas o documentos administrativos introduce problemas de seguridad de la información.

Restricciones de naturaleza estratégica

Las restricciones se pueden originar en cambios planificados o posibles en la orientación o la estructura de la organización. Se expresan en los planes operativos o estratégicos de la organización.

Por ejemplo, la cooperación internacional al compartir información sensible puede hacer que se requieran acuerdos relacionados con el intercambio seguro.

Restricciones territoriales

La estructura y/o el propósito de la organización pueden introducir restricciones específicas tales como la distribución de las sedes en todo el territorio nacional o en el extranjero.

Los ejemplos incluyen servicios postales, embajadas, bancos, subsidiarias de un grupo industrial grande, etc.

Restricciones que se originan en el clima político y económico

El funcionamiento de una organización puede sufrir cambios profundos debido a eventos específicos tales como huelgas o crisis nacionales e internacionales.

Por ejemplo, algunos servicios deberían ser continuos, incluso durante una crisis grave.

Restricciones estructurales

La naturaleza de la estructura de una organización (divisional, funcional u otras) puede llevar a que la política específica de seguridad de la información y la organización de la seguridad se adapten a la estructura.

Por ejemplo, una estructura internacional debería poder aceptar los requisitos de seguridad específicos para cada país.

Restricciones funcionales

Las restricciones funcionales se originan directamente en las misiones específicas o generales de la organización.

Por ejemplo, una organización que funciona las 24 horas del día debería garantizar que sus recursos estén disponibles continuamente.

Restricciones relacionadas con el personal

La naturaleza de estas restricciones varía considerablemente. Ellas están ligadas a: nivel de responsabilidad, contratación, calificación, entrenamiento, concienciación sobre la seguridad, motivación, disponibilidad, etc.

Por ejemplo, la totalidad del personal de una organización de defensa debería tener la autorización para manejar información altamente confidencial.

Restricciones que se originan en el calendario de la organización

Estas restricciones pueden ser el resultado de la reestructuración o el establecimiento de políticas nacionales o internacionales que impone fechas límites determinadas.

Por ejemplo, la creación de una división de seguridad.

Restricciones relacionadas con los métodos

Será necesario que métodos adecuados para los conocimientos de la organización se impongan para aspectos tales como planificación de proyectos, especificaciones, desarrollo, etc.

Por ejemplo, una restricción típica 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 llevado a una "cultura" específica dentro de la organización, la cual puede ser incompatible con los controles de seguridad. Esta cultura es el marco general de referencia del personal y puede estar determinada por muchos aspectos que incluyen educación, instrucción, experiencia profesional, experiencia fuera del trabajo, opiniones, filosofía, creencias, status social, etc.

Restricciones de presupuesto

Los controles recomendados para la seguridad puede en ocasiones tener un costo muy alto. Aunque no siempre es conveniente basar las inversiones de seguridad en la relación costo-eficacia, generalmente el departamento financiero de la organización exige una justificación económica.

Por ejemplo, en el sector privado y algunas organizaciones públicas, el costo total de los controles de seguridad no debería exceder al costo de las consecuencias potenciales de los riesgos. Por ende, la alta gerencia debería evaluar y tomar riesgos calculados si quiere evitar los costos de seguridad excesivos.

A.3 LISTADO DE LAS REFERENCIAS LEGISLATIVAS Y REGLAMENTARIAS QUE SE APLICAN A LA ORGANIZACIÓN

Los requisitos reglamentarios que se aplican a la organización deberían estar identificados. Estos pueden ser leyes, decretos, reglamentos específicos en el campo de la organización o reglamentos internos/externos. Esto también involucra contratos y acuerdos y, de forma más general, todas las obligaciones de naturaleza legal o reglamentaria.

A.4 LISTADO DE LAS RESTRICCIONES QUE AFECTAN AL ALCANCE

Al identificar las restricciones, es posible hacer un listado de aquellas que tienen un impacto en el alcance y determinar cuáles son, no obstante, viables para la acción. Estas se añaden y, posiblemente enmienden, a las restricciones de la organización determinadas anteriormente. Los siguientes párrafos representan un listado no exhaustivo de los posibles tipos de restricciones.

Restricciones que se originan en procesos preexistentes

Los proyectos de aplicación no necesariamente se desarrollan simultáneamente. Algunos dependen de procesos ya existentes. Aunque un proceso se puede dividir en subprocesos, el proceso no necesariamente tiene influencia de todos los subprocesos de otro proceso.

Restricciones técnicas

Las restricciones técnicas, relacionadas con la infraestructura, en general se originan del hardware y software instalados, y en los recintos o los lugares que albergan a los procesos:

- archivos (requisitos relacionados con la organización, la gestión de los medios, la gestión de las reglas de acceso, etc.)

- arquitectura general (requisitos relacionados con la topología (centralizada, distribuida, cliente-servidor), arquitectura física, etc.)

- software de aplicación (requisitos relacionados con el diseño de software específico, normas de mercado, etc.)

- paquetes de software (requisitos relacionados con normas, nivel de evaluación, calidad, conformidad con las normas, seguridad, etc.)

- hardware (requisitos relacionados con normas, calidad, conformidad con las normas, etc.)

- redes de comunicación (requisitos relacionados con cobertura, normas, capacidad, confiabilidad, etc.)

- infraestructura de la edificación (requisitos relacionados con ingeniería civil, construcción, altas tensiones, bajas tensiones, etc.)

Restricciones financieras

La implementación de los controles de seguridad con frecuencia está restringida por el presupuesto que la organización puede comprometer. Sin embargo, las restricciones financieras deberían ser las últimas en considerarse dado que la distribución de presupuesto para la seguridad de puede negociar con base en el estudio de seguridad.

Restricciones ambientales

Las restricciones ambientales se originan en el ambiente geográfico o económico en el cual se implementan los procesos: país, clima, riesgos naturales, situación geográfica, clima económico, etc.

Restricciones de tiempo

El tiempo que se requiere para implementar los controles de seguridad se debería considerar con respecto a la capacidad de actualizar el sistema de información; si el tiempo para la implementación es muy prolongado, los riesgos para los cuales se diseñó el control pueden haber cambiado. El tiempo es un factor determinante para la selección de soluciones y prioridades.

Restricciones relacionadas con los métodos

Se deberían utilizar métodos adecuados para los conocimientos de la organización para la planificación de proyectos, especificaciones, desarrollo, etc.

Restricciones organizacionales

Varias restricciones se pueden deducir de los requisitos organizacionales:

- funcionamiento (requisitos relacionados con tiempos de entrega, suministro de servicios, vigilancia, monitoreo, planes de emergencia, funcionamiento degradado, etc.)

- mantenimiento (requisitos para la detección y solución de incidentes, acciones preventivas, corrección rápida, etc.)

- gestión de recursos humanos (requisitos relacionados con entrenamiento del operario y el usuario, calificación para cargos tales como administrador del sistema o administrador de datos, etc.)

- gestión administrativa (requisitos relacionados con las responsabilidades, etc.)

- gestión del desarrollo (requisitos relacionados con herramientas para el desarrollo, ingeniería de software ayudada con computador, planes de aceptación, organización que se va a establecer, etc.)

- gestión de las relaciones externas (requisitos relacionados con la organización de las relaciones con terceras partes, contratos, etc.)

ANEXO B
(Informativo)

IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS Y EVALUACIÓN DEL IMPACTO

B.1 EJEMPLOS DE IDENTIFICACIÓN DE LOS ACTIVOS

Para realizar la valoración de los activos, es necesario que la organización identifique primero sus activos (con un grado adecuado de detalles). Se pueden diferenciar dos clases de activos.

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

B.1.1 Identificación de los activos primarios

Para describir el alcance de manera más precisa, esta actividad consiste en la identificación de los activos primarios (actividades y procesos del negocio, información). Esta identificación es realizada por un grupo de trabajo mixto que representa al proceso (directores, especialistas en sistema de información y usuarios).

Por lo general, los activos primarios son los procesos y la información centrales de la actividad en el alcance. También se pueden considerar otros activos primarios tales como los procesos de la organización, que serán más convenientes para elaborar una política de seguridad de la información o un plan de continuidad del negocio. Dependiendo del propósito, algunos estudios no exigen un análisis exhaustivo de todos los elementos que constituyen el alcance. En tales casos, las fronteras del estudio pueden estar limitadas a los elementos clave del alcance.

Los activos primarios son de dos tipos:

1) Procesos (o subprocesos) y actividades del negocio, por ejemplo

- procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización;
- procesos que contienen procesos secretos o que implican tecnología de propietario;
- procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización;
- procesos que son necesarios para que la organización cumpla con requisitos contractuales, legales o reglamentarios.

2) Información

De forma más general, la información primaria comprende principalmente:

- información vital para la ejecución de la misión o el negocio de la organización;
- información personal que se puede definir específicamente en el sentido de las leyes nacionales relacionadas con la privacidad;
- información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas;
- información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición.

Los procesos y la información que no se identifican como sensibles después de esta actividad, no tendrán una clasificación definida en el resto del estudio. Esto significa que incluso si tales procesos o información se ven comprometidos, la organización aún cumplirá la misión de manera exitosa.

No obstante, estos procesos e información con frecuencia heredan controles implementados para proteger los procesos y la información identificados como sensibles.

B.1.2 Listado y descripción de los activos de soporte

El alcance consiste en activos que se deberían identificar y describir. Estos activos tienen vulnerabilidades que son explotables por las amenazas cuya meta es deteriorar los activos primarios del alcance (procesos e información). Estos son de varios tipos:

Hardware

Este tipo consta de todos los elementos físicos que dan soporte a los procesos.

Equipo de procesamiento de datos (activo)

Equipo automático de procesamiento de información que incluye los elementos que se requieren para funcionar independientemente.

Equipo transportable

Equipo de computación portátil.

EJEMPLOS Computador laptop, asistente digital personal (PDA).

Equipo fijo

Equipo de computación utilizado en las instalaciones de la organización.

EJEMPLOS Servidor, microcomputador utilizado como estación de trabajo.

Periféricos para procesamiento

Equipo conectado a un computador a través de un puerto de comunicaciones (conexión en serie, paralela, etc.) para ingresar, transportar o transmitir datos.

EJEMPLOS Impresora, unidad de disco removible.

Medios para datos (pasivo)

Estos son los medios para almacenamiento de datos o funciones.

Medio electrónico

Medio de información que se puede conectar a un computador o una red de computadores para el almacenamiento de datos. Independientemente de su tamaño compacto, estos medios pueden contener una gran cantidad de datos. Se pueden utilizar con equipo de computación normal.

EJEMPLOS Disquetes, CD-ROM, cartucho de soporte, disco duro removible, clave de memoria, cinta.

Otros medios

Medios estáticos, no electrónicos que contienen datos.

EJEMPLOS Papel, diapositivas, transparencias, documentación, fax.

Software

El software consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos.

Sistema operativo

Este incluye todos los programas de un computador que constituyen la base operativa desde la cual se ejecutan todos los otros programas (servicios o aplicaciones). Incluye un núcleo y servicios o funciones básicas. Dependiendo de la arquitectura, un sistema operativo puede ser monolítico o estar constituido por un micronúcleo y un conjunto de servicios del sistema. Los elementos principales del sistema operativo son los servicios de administración del equipo (CPU, memoria, disco e interfaces de red), servicios para la administración de tareas o procesos y servicios de administración de los derechos de usuario.

Software de servicio, mantenimiento o administración

Software que se caracteriza por el hecho de que complementa los servicios del sistema operativo y no está directamente al servicio de los usuarios ni las aplicaciones (aunque usualmente es esencial o incluso indispensable para la operación global del sistema de información).

Paquetes de software o software estándar

El software estándar o los paquetes de software son productos completos comercializados como tales (a diferencia de los desarrollos únicos o específicos) con medios, divulgación y mantenimiento. Suministra servicios para los usuarios y las aplicaciones, pero no son personalizados ni específicos de la manera en que los son las aplicaciones del negocio.

EJEMPLOS Software para el manejo de la base de datos, software de mensajería electrónica, software de grupos, software de directorio, software para servidor web, etc.

Aplicaciones del negocio

Aplicación estándar del negocio

Este es un software comercial diseñado para brindar a los usuarios acceso directo a los servicios y las funciones que ellos necesitan de su sistema de información en su contexto profesional. Existe un rango de campos muy amplio, teóricamente ilimitado.

EJEMPLOS Software de contabilidad, software para el control de herramientas para máquinas, software para cuidado del cliente, software para la gestión de la competencia del personal, software administrativo, etc.

Aplicación específica del negocio

Este es un software en el cual se han desarrollado específicamente varios aspectos (soporte primario, mantenimiento, mejora, etc.) para brindar a los usuarios acceso directo a los servicios y las funciones que ellos necesitan de su sistema información. Existe un rango de campos muy amplio, teóricamente ilimitado.

EJEMPLOS Gestión de facturación de los clientes de los operadores de telecomunicaciones, aplicación de monitoreo en tiempo real para lanzamiento de cohetes.

Red

El tipo de red consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información.

Medios y soportes

Los medios o el equipo de comunicaciones y telecomunicaciones se caracterizan principalmente por los rasgos físicos y técnicos del equipo (punto a punto, difusión)

y por los protocolos de comunicación (vínculo o red - niveles 2 y 3 del modelo OSI de 7 capaz o estratos).

Ejemplos: red pública de conmutación telefónica (PSTN), Ethernet, GigabitEthernet, línea de suscriptor digital asimétrica (ADSL), especificaciones de protocolo inalámbrico (por ejemplo WiFi 802.11), Bluetooth, FireWire.

Relevos pasivos o activos

Este subtipo incluye todos los dispositivos que no son las terminaciones lógicas de las comunicaciones (visión del sistema de información), sino que son dispositivos intermedios o de relevo. Los relevos se caracterizan por los protocolos de comunicaciones de red soportada. Además de relevo básico, con frecuencia incluyen funciones y servicios de enrutamiento y/o filtro, que emplean interruptores de comunicación y enrutadores con filtros. A menudo se puede administrar de forma remota y por lo común tienen la capacidad para generar registros.

EJEMPLOS Puente, enrutador, hub, interruptor, intercambio automático.

Interfaz de comunicación

Las interfaces de comunicación de las unidades de procesamiento se conectan a las unidades de procesamiento pero se caracterizan por los medios y los protocolos soportados, por cualquier filtración instalada, funciones de generación de registros o advertencias y sus capacidades, y por la probabilidad y el requisito de administración remota.

EJEMPLOS Servicio general del paquete de radio (GPRS), adaptador de Ethernet.

Personal

Este tipo consiste en todos los grupos de personas involucradas en el sistema de información.

Persona a cargo de la toma de decisiones

Las personas a cargo de tomar las decisiones son los propietarios de los activos primarios (información y funciones) y los directores de la organización o el proyecto específico.

EJEMPLOS Alta gerencia, líder de proyectos.

USUARIOS

Los usuarios son las personas que manejan los elementos sensibles en el contexto de su actividad y quienes tienen una responsabilidad especial a este respecto. Pueden tener derechos especiales de acceso al sistema de información para realizar sus labores diarias.

EJEMPLOS Gestión de recursos humanos, gestión financiera, gerente de riesgos.

Personal de operación/mantenimiento

Son las personas a cargo de la operación y mantenimiento del sistema de información. Tienen derechos especiales de acceso al sistema de información para realizar sus labores diarias.

EJEMPLOS Administrador del sistema, administrador de datos, funcionarios a cargo de copias de seguridad, escritorio de ayuda, operadores del despliegue de la aplicación, funcionarios de seguridad.

Desarrolladores

Ellos están a cargo del desarrollo de las aplicaciones de la organización. Tienen acceso a parte del sistema de información con derechos de alto nivel pero no toman ninguna acción sobre los datos de producción.

EJEMPLOS Desarrolladores de la aplicación del negocio.

Sitio

Este tipo comprende todos los lugares que contienen el alcance o parte de éste, y los medios físicos que se requieren para su funcionamiento.

Ubicación

Ambiente externo

Involucra todos los lugares en los cuales no se pueden aplicar los medios de seguridad de la organización.

EJEMPLOS Domicilios del personal, instalaciones de otra organización, ambiente hubiera del sitio (área urbana, área de peligro).

Instalaciones

Este lugar está limitado por el perímetro de la organización que está en contacto directo con el exterior. Puede tratarse de una frontera protectora física creada con barreras físicas o medios de vigilancia alrededor de las edificaciones.

EJEMPLOS Establecimiento, edificaciones.

Zona

Una zona está formada por una frontera protectora física que forma divisiones dentro de las instalaciones de la organización. Se crear con barreras físicas alrededor de las infraestructuras de procesamiento de información de la organización.

EJEMPLOS Oficinas, zona de acceso reservado, zona segura.

Servicios esenciales

Todos los servicios que se requieren para que funcione el equipo de la organización.

Comunicación

Los servicios y el equipo de telecomunicaciones suministrados por un operador.

EJEMPLOS Línea telefónica, PABX, redes telefónicas internas.

Servicios públicos

Servicios y medios (fuentes de suministro e instalaciones eléctricas) que se requieren para brindar energía eléctrica a los equipos y los periféricos de tecnología de la información.

EJEMPLOS Suministro de energía de baja tensión, inversor, cabeza de distribución del circuito eléctrico.

Suministro de agua

Disposición de residuos

Servicios y medios (equipo, control) para refrigeración y purificación del aire.

EJEMPLOS Acondicionadores de aire, tuberías para agua fría.

Organización

Este tipo describe la estructura organizacional, que consta de todas las estructuras del personal asignado a una labor y los procedimientos que controlan tales estructuras.

Autoridades

Estas son organizaciones de las cuales la organización estudiada deriva su autoridad. Pueden estar afiliadas legalmente o ser externas. Ellas imponen restricciones a la organización estudiada en términos de reglamentos, decisiones y acciones.

EJEMPLOS Organismo administrativo, oficina principal de un organización.

Estructura de la organización

Consiste en las diversas ramas de la organización, incluyendo sus actividades funcionales cruzadas, bajo el control de su gerencia.

EJEMPLOS Gestión de recursos humanos, gestión de tecnología de la información gestión de compras, gestión de las unidades de negocios, servicio de seguridad de la edificación, servicio de incendios, gestión de auditorías.

Organización del sistema o el proyecto

Involucra la organización establecida para un proyecto o servicio específicos.

EJEMPLOS Proyecto de desarrollo de una aplicación nueva, proyecto de migración del sistema de información.

Subcontratistas/proveedores/fabricantes

Estas son entidades que suministran a la organización un servicio o los recursos y se obligan mediante contratos.

EJEMPLOS compañía de gestión de las instalaciones, compañía de contratación externa, compañías de consultoría.

B.2 VALORACIÓN DE LOS ACTIVOS

El paso siguiente a la identificación de los activos es pactar la escala que se va a utilizar y los criterios para la asignación de una ubicación particular en esa escala para cada uno de los activos, con base en la valoración. Debido a la diversidad de activos que se encuentran en la mayoría de los organizaciones, es probable que algunos activos que

tengan un valor monetario conocido sean valorados en la moneda local en donde están presentes, mientras otros que tiene un valor más cualitativo se les puede asignar un rango de valores, por ejemplo, desde "muy bajo" hasta "muy alto". La decisión de utilizar una escala cuantitativa en lugar de una cualitativa es realmente un asunto de preferencia organizacional, pero debería ser pertinente para los activos que se están valorando. Ambos tipos de valoración se pueden utilizar para el mismo activo.

Los términos típicos utilizados para la valoración cualitativa de los activos incluyen palabras como: insignificante, muy bajo, bajo, medio, alto, muy alto y crítico. La selección y la gama de términos adecuados para una organización dependen significativamente de las necesidades de seguridad , del tamaño y de otros factores específicos para dicha organización.

Criterios

Los criterios utilizados como base para asignar un valor a cada uno de los activos se deberían redactar en términos que no sean ambiguos. Éste es a menudo uno de los aspectos más difíciles de la valoración de los activos puesto que los valores de algunos de ellos pueden estar determinados de manera subjetiva y probablemente muchos individuos diferentes estén realizando la determinación. Los posibles criterios empleados para determinar el valor de un activo incluyen su costo original, su costo de reposición o renovación, o su valor puede ser abstracto, por ejemplo el valor de la reputación de una organización.

Otra base para la valoración de los activos es el costo en que se incurre debido a la pérdida de confidencialidad, integridad y disponibilidad como resultado de un incidente. El no repudio, la obligación de rendir cuentas, la autenticidad y la confiabilidad también se deberían considerar, según corresponda. Dicha valoración proporcionaría las dimensiones que tienen los elementos importantes para el valor del activo, además del costo de reposición, con base en estimaciones de las consecuencias adversas para el negocio que se producirían debido a los incidentes de seguridad dentro de un conjunto determinado de circunstancias. Se hace énfasis en que este enfoque explica las consecuencias que es necesario factorizar en la evaluación del riesgo.

Es posible que muchos activos durante el transcurso de la valoración tengan varios valores asignados. Por ejemplo: un plan de negocios puede ser valorado con base en la labor que se requiere para desarrollar el plan, podría ser valorado con base en la labor para ingresar los datos y también con base en su valor para un competidor. Es probable que cada uno de los valores asignados tenga diferencias considerables. El valor asignado puede ser el máximo de todos los valores posibles o puede ser la suma de algunos o todos los valores posibles. En el análisis final, es necesario determinar cuidadosamente el valor o los valores que se asignan a un activo determinado ya que el valor final asignado ingresa en la determinación de los recursos que se van a utilizar para la protección de ese activo.

Reducción hasta la base común

En última instancia, es necesario reducir todas las valoraciones de los activos hasta una base común. Esto se puede hacer con la ayuda de criterios como los que se indican a continuación. Los criterios que se pueden utilizar para evaluar las consecuencias posibles resultantes de la pérdida de confidencialidad, integridad, disponibilidad, no repudio,

responsabilidad, autenticidad o confiabilidad de los activos son:

- incumplimiento de la legislación y/o reglamentación;
- deterioro en el desempeño del negocio;
- pérdida del buen nombre/efecto negativo en la reputación;
- brechas asociadas con la información personal;
- efectos adversos en el cumplimiento de la ley;
- brechas en la confidencialidad;
- brechas de orden público;
- pérdida financiera;

- alteración de las actividades del negocio;
- hacer peligrar la seguridad ambiental.

Otro enfoque para evaluar las consecuencias podría ser:

- Interrupción de servicios.
    - Incapacidad para prestar el servicio.
- Pérdida de la confianza del cliente.
    - Pérdida de credibilidad en el sistema información interno.
    - Daño en la reputación.
- Alteración de la operación interna.
    - Alteración en la propia organización.
    - Costo interno adicional.
- Alteración en la operación de una tercera parte.
    - Alteración de las terceras partes que tienen transacciones con la organización.
    - Diversos tipos de agravios.
- Contravenciones de leyes/reglamentos:
    - Incapacidad para cumplir las obligaciones legales.
- Incumplimiento de contrato:
    - Incapacidad para cumplir las obligaciones contractuales.
- Peligro para el personal/seguridad del usuario:
    - Peligro para el personal de la organización y/o los usuarios.
- Ataque a la vida privada de los usuarios.
- Pérdidas financieras.
- Costo financiero para emergencias o reparaciones:
- en términos de personal,
- en términos de equipo,

- en términos de estudios, informes de expertos.
- Pérdida de mercancías/fondos/activos.
- Pérdida de clientes, pérdida de proveedores.
- Procesos judiciales y castigos.
- Pérdida de una ventaja competitiva.
- Pérdida de liderazgo tecnológico/técnico.
- Pérdida de eficacia/confianza.
- Pérdida de reputación técnica.
- Debilidad en la capacidad de negociación.
- Crisis industrial (huelgas).
- Crisis del gobierno.
- Despidos.
- Daños materiales.

Estos criterios son ejemplos de aspectos que se deben considerar para la valoración de los activos. Con el fin de llevar a cabo las valoraciones, es necesario que la organización seleccione los criterios que son pertinentes para su tipo de negocios y sus requisitos de seguridad. Ello podría implicar que algunos de los criterios indicados anteriormente no sean aplicables, y que puede ser necesario añadir otros a este listado.

Escala

Después de establecer los criterios que se van a considerar, la organización debería pactar la escala que se va a utilizar en toda la organización. El primer paso es decidir sobre la cantidad de niveles que se van a emplear. No existen reglas con respecto a la cantidad de niveles que sea más adecuada. Más niveles brindan un mayor grado de granulosidad pero en ocasiones una diferenciación demasiado fina dificulta hacer asignaciones consistentes en toda la organización. Normalmente, cualquier número de niveles entre 3 (por ejemplo, bajo, medio y alto) y 10 se puede utilizar siempre que sea consistente con el enfoque que la organización utiliza para todo el proceso de evaluación de riesgos.

Una organización puede definir sus propios límites para los valores de los activos, como "bajo", "medio" o "alto". Estos límites se deberían evaluar de acuerdo con los criterios seleccionados (por ejemplo, para pérdida financiera potencial, se deberían dar en valores monetarios, pero para consideraciones tales como peligro para la seguridad del personal, la valoración monetaria puede ser compleja y no adecuada para todas las

organizaciones). Finalmente, depende totalmente de la organización decidir acerca de 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 organización muy grande.

Dependencias

Cuanto más pertinentes y numerosos sean los procesos del negocio soportados por un activo, mayor es el valor de este activo. Es recomendable identificar las dependencias de los activos en los procesos del negocio y otros activos ya que esto puede tener influencia en los valores de los activos. Por ejemplo, la confidencialidad de los datos se debería conservar durante todo su ciclo vital, en todas las etapas, incluyendo almacenamiento y procesamiento, es decir que las necesidades de la seguridad para el almacenamiento de los datos y los programas de procesamiento se debería relacionar directamente con el valor que representa la confidencialidad de los datos almacenados y procesados. De igual manera, si un proceso del negocio depende de la integridad de determinados datos que produce un programa, los datos de entrada de este programa deberían tener una confiabilidad adecuada. Además, la integridad de la información dependerá del hardware y el software utilizados para su almacenamiento y procesamiento. También, el hardware dependerá del suministro de energía eléctrica y, tal vez, del aire acondicionado. De este modo, la información acerca de las dependencias facilitará la identificación de las amenazas y particularmente de las vulnerabilidades. Igualmente, ayudará a garantizar que se da el valor verdadero a los activos (a través de las relaciones de dependencias), indicando así el nivel conveniente de protección.

Los valores de los activos de los cuales dependen otros activos se pueden modificar de la siguiente manera:

- si los valores de los activos dependientes (por ejemplo los datos) son menores o iguales al valor del activo considerado (por ejemplo el software), su valor permanece igual;

- si los valores de los activos dependientes (por ejemplo, los datos) son mayores, entonces el valor del activo considerado (por ejemplo, el software) se deberían incrementar de acuerdo con:

    - el grado de dependencias;

    - los valores de los otros activos.

Una organización puede tener algunos valores que están disponibles más de una vez, como por ejemplo las copias de los programas de software o el mismo tipo de computador utilizado en la mayoría de las oficinas. Es importante considerar este factor cuando se hace la valoración de los activos. Por una parte, estos valores pueden ser omitidos con facilidad, por lo tanto es necesario tener precaución para identificarlos en su totalidad; por otra parte, se pueden utilizar para reducir los problemas de disponibilidad.

Salida

La salida final de este paso es un listado de los activos y sus valores con relación a la

divulgación (preservación de la confidencialidad), la modificación (preservación de la integridad, autenticidad, no repudio y responsabilidad), no disponibilidad y destrucción (preservación de la disponibilidad y la confiabilidad) y al costo del reemplazo.

B.3 EVALUACIÓN DEL IMPACTO

Un incidente en la seguridad de la información puede tener impacto en más de uno de los activos o únicamente en una parte de uno de los activos. El impacto se relaciona con el grado de éxito del incidente. En consecuencia, existe una diferencia importante entre el valor del activo y el impacto resultante de un incidente. Se considera que el impacto tiene un efecto inmediato (operacional) o un efecto futuro (en el negocio) que incluye consecuencias financieras y de mercado.

El impacto inmediato (operacional) es director o indirecto.

Directo:

a) El valor financiero del reemplazo del activo perdido (o parte de este activo).

b) El costo de adquisición, configuración e instalación del activo nuevo o de su copia de soporte.

c) El costo de las operaciones suspendidas debido al incidente hasta que se restaure el servicio prestado por el (los) activo (s).

d) El impacto tiene como resultado una brecha en la seguridad de la información.

Indirecto:

a) Costos de la oportunidad (nuevos recursos financieros necesarios para reemplazar o reparar un activo se podrían haber utilizado en otra parte).

b) El costo de las operaciones interrumpidas.

c) El potencial de la mala utilización de la información obtenida a través de una brecha en la seguridad.

d) Incumplimiento de las obligaciones estatutarias o reglamentarias.

e) Incumplimiento del código ético de conducta.

Así, la primera evaluación (sin controles de ningún tipo) estimará un impacto como muy cercano al valor del activo involucrado (o combinación de valores). Para toda repetición posterior para este activo, el impacto será diferente (normalmente más bajo) dada la presencia y la eficacia de los controles implementados.

ANEXO C
(Informativo)

EJEMPLOS DE AMENAZAS COMUNES

La siguiente tabla presenta ejemplos de amenazas comunes. La lista se puede utilizar durante el proceso de evaluación de las amenazas. Ellas pueden ser deliberadas, accidentales o ambientales (naturales) y pueden dar como resultado, por ejemplo, daño o pérdida de los servicios esenciales. Para cada uno de los tipos de amenazas, la siguiente lista indica los casos en que D (deliberadas), A (accidentales) y E (ambientales) son pertinentes. La letra D se utiliza para todas las acciones deliberadas que tienen como objetivo los activos de la información, A se utiliza para las acciones humanas que pueden dañar accidentalmente los activos de información y E se utiliza para todos los incidentes que no se basa en las acciones humanas. Los grupos de amenazas no están en orden de prioridad.

Tipo	Amenazas	Origen
Daño físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha subrepticia	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D

	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Se recomienda poner atención particular a las fuentes de amenazas humanas. Éstas se desglosan específicamente en la siguiente tabla:

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería social • Intrusión, accesos forzados al sistema • Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador (por ejemplo, espionaje cibernético) • Acto fraudulento (por ejemplo, repetición, personificación, interceptación) • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/terrorismo • Guerra* (warfare) de información • Ataques contra el sistema (por ejemplo, negación distribuida del servicio) • Penetración en el sistema • Manipulación del sistema
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja Política • Explotación económica • Hurto de información • Intrusión en la privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales) por ejemplo, error en el ingreso de los datos,	• Asalto a un empleado • Chantaje • Observar información de propietario • Abuso del computador • Soborno de información • Ingreso de datos falsos o corruptos

	error de programación)	• Interceptación • Código malintencionado (por ejemplo, virus, bomba lógica, caballo troyano) • Venta de información personal • Errores* (bugs) en el sistema • Sabotaje del sistema • Acceso no autorizado al sistema

ANEXO D
(Informativo)

VULNERABILIDADES Y MÉTODOS PARA LA EVALUACIÓN DE LA VULNERABILIDAD

D.1 EJEMPLOS DE VULNERABILIDADES

La siguiente tabla presenta ejemplos de las vulnerabilidades en diversas áreas de seguridad, e incluye ejemplos de amenazas pueden explotar estas vulnerabilidades la lista puede brindar ayuda durante la evaluación de las amenazas y vulnerabilidades, con el fin de determinar los escenarios pertinentes de incidente. Se hace énfasis en que en algunos casos otras amenazas también pueden tomar ventaja de estas vulnerabilidades.

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Falta de pruebas de auditoría	Abuso de los derechos
	Distribución errada de los derechos de acceso	Abuso de los derechos
	Software de distribución amplia	Corrupción de datos
	Utilización de los programas de aplicación a los datos errados en términos de tiempo	Corrupción de datos
	Interfase de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso

	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Software	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Falta de control eficaz del cambio	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Falta de copias de respaldo	Manipulación con software
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Falta de prueba del envío o la recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha subrepticia
	Tráfico sensible sin protección	Escucha subrepticia
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Falta de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas autorizadas	Espionaje remoto
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios

	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos
	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos
	Falta de auditorías (supervisiones) regulares	Abuso de los derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de los derechos
	Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento del sistema de información
	Falta de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Falta de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Falta de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Falta de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Falta de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Falta de planes de continuidad	Falla del equipo
	Falta de políticas sobre el uso del correo electrónico	Error en el uso
	Falta de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Falta de registros en las bitácoras*(logs) de administrador y operario.	Error en el uso
	Falta de procedimientos para el manejo de información clasificada	Error en el uso
	Falta de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos

	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Falta de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Falta de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Falta de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Falta de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Falta de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

D.2 MÉTODOS PARA LA EVALUACIÓN DE LAS VULNERABILIDADES TÉCNICAS

Se pueden utilizar métodos proactivos tales como los ensayos del sistema de información para identificar las vulnerabilidades que dependen de la importancia del sistema de tecnología de información y telecomunicaciones (TIC), y los recursos disponibles (por ejemplo, fondos asignados, tecnología disponible, personas con las habilidades para realizar ensayos). Los métodos de ensayo incluyen los siguientes:

- herramienta automática de exploración de la vulnerabilidad;
- ensayo y evaluación de la seguridad;
- ensayo de penetración;
- revisión del código.

La herramienta automática de exploración de la vulnerabilidad se utiliza para explorar un grupo de anfitriones (hosts)* o una red para servicios vulnerables conocidos (por ejemplo, el sistema permite el protocolo de transferencia de archivos (FTP) anónimo, el relevo* (relaying) de envío de correo). Conviene anotar, sin embargo, que algunas de las vulnerabilidades potenciales identificadas por la herramienta automática de exploración

pueden no representar vulnerabilidades reales en el contexto del entorno del sistema. Por ejemplo, algunas de estas herramientas de exploración clasifican las vulnerabilidades potenciales sin tener en cuenta el entorno y los requisitos del lugar. Algunas de las vulnerabilidades identificadas por el software automático de exploración pueden en realidad no ser vulnerables para un lugar particular pero se pueden configurar de esa manera debido a que su entorno lo exige. De este modo, este método de ensayo puede producir falsos positivos.

El ensayo y la evaluación de la seguridad es otra técnica que se puede utilizar para identificar vulnerabilidades en el sistema TIC durante el proceso de evaluación del riesgo. Incluye el desarrollo y la ejecución de un plan de ensayo (por ejemplo, macro de ensayo, procedimientos de ensayo y resultados esperados del ensayo). El propósito del ensayo de la seguridad del sistema es probar la eficacia de los controles de seguridad de un sistema TIC en la medida en que se apliquen en un entorno operativo. El objetivo es garantizar que los controles que se aplican satisfacen la especificación aprobada de seguridad para el software y el hardware, e implementar la política de seguridad de la organización o cumplir las normas de la industria.

El ensayo de penetración se puede utilizar para complementar la revisión de los controles de seguridad y garantizar que las diversas facetas del sistema TIC están aseguradas. El ensayo de penetración, cuando se utiliza en el proceso de evaluación de riesgos, se puede utilizar para evaluar la capacidad del sistema TIC para tolerar intentos intencionales de burlar la seguridad del sistema. Su objetivo es someter a ensayo el sistema TIC desde el punto de vista de la fuente de una amenaza e identificar las fallas potenciales en los esquemas de protección del sistema.

La revisión del código es la forma más exhaustiva (pero también la más costosas) de evaluación de la vulnerabilidad.

Los resultados de estos tipos de ensayos de la seguridad ayudarán a identificar las vulnerabilidades del sistema.

Es importante anotar que las herramientas y técnicas de penetración pueden dar resultados falsos, a menos que la vulnerabilidad sea explotada exitosamente. Para explotar vulnerabilidades particulares, es necesario conocer el sistema/la aplicación/los parches exactos establecidos en el sistema que se somete a ensayo. Si no se conocen estos datos en el momento del ensayo, podría no ser posible explotar de manera exitosa la vulnerabilidad particular (por ejemplo, llegar a una cápsula inversa remota)*; sin embargo, aún es posible detener o reiniciar un proceso o sistema ensayado. En tal caso, el objeto ensayado se debería considerar también vulnerable.

Los métodos pueden incluir las siguientes actividades:

- entrevistas a personas y usuarios;
- cuestionarios;
- inspección física;
- análisis de documentos.

PROYECTO DE
NORMA TÉCNICA COLOMBIANA NTC-ISO 27005 DE 174/08

ANEXO E
(Informativo)

ENFOQUES PARA LA EVALUACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

E.1 EVALUACIÓN DE ALTO NIVEL DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

La evaluación de alto nivel permite la definición de las prioridades y la cronología de las acciones. Por varias razones, tales como el presupuesto, puede no ser posible implementar todos los controles simultáneamente y únicamente se pueden atender los riesgos más críticos a través del proceso de tratamiento de riesgos. De igual modo, puede ser prematuro iniciar una gestión detallada del riesgo si la implementación sólo se puede dar después de uno o dos años. Para lograr este objetivo, la evaluación de alto nivel puede empezar con una evaluación de alto nivel de las consecuencias en lugar de empezar con un análisis sistemático de amenazas, vulnerabilidades, activos y consecuencias.

Otra razón para empezar la evaluación de alto nivel es sincronizar con otros planes relacionados con la gestión de cambios (o continuidad del negocio). Por ejemplo, no está bien asegurar completamente un sistema o aplicación si se planifica subcontratarla en el futuro cercano, aunque aún puede valer la pena hacer la evaluación de riesgos con el fin de definir el contrato de subcontratación.

Las características de la repetición de la evaluación de riesgos de alto nivel pueden incluir las siguientes:

- la evaluación de alto nivel de los riesgos puede abordar una visión más global de la organización y su sistema de información, considerando los aspectos tecnológicos como dependientes de los aspectos del negocio. Al hacer esto, el análisis del contexto se concentra más en el negocio y el ambiente operativo que en los elementos tecnológicos;

- la evaluación de alto nivel de los riesgos puede abordar una lista más limitada de amenazas y vulnerabilidades agrupadas en dominios definidos o apresurar el proceso, puede enfocarse en riesgos o escenarios de ataque en lugar de sus elementos;

- los riesgos representados en una evaluación de alto nivel de los riesgos con frecuencia son dominios de riesgo más generales que riesgos específicos identificados. Dado que los escenarios o las amenazas se agrupan en dominios, el tratamiento del riesgo propone listas de controles en este dominio. Las actividades de tratamiento del riesgo intentan primero proponer y seleccionar controles comunes que sean válidos a través de todo el sistema;

- sin embargo, la evaluación de alto nivel de los riesgos, debido a que pocas veces aborda los detalles tecnológicos, es más adecuada para proporcionar controles organizacionales y no técnicos y aspectos de gestión de los controles técnicos, o

salvaguardas técnicas claves y comunes como por ejemplo los antivirus y las copias de respaldo.

Las ventajas de una evaluación de alto nivel de los riesgos son las siguientes:

- la incorporación de un enfoque inicial sencillo probablemente tenga aceptación del programa de evaluación de riesgos;

- sería posible construir un panorama estratégico de un programa de seguridad de la información en la organización, es decir, actuaría como una buena ayuda de planificación;

- los recursos y el dinero se pueden aplicar donde son de más beneficio, y se tratarían primero los sistemas que probablemente tenga mayor necesidad de protección.

Dado que los análisis iniciales de riesgos son de alto nivel y potencialmente menos exactos, la única desventaja potencial es que puede no identificarse algunos procesos o sistemas del negocio que requieren de una segunda evaluación detallada del riesgo. Esto se puede evitar si existe información adecuada sobre todos los aspectos de la organización y sus sistemas e información, incluyendo la información obtenida de la evaluación de los incidentes de seguridad en la información.

La evaluación de alto nivel de los riesgos toma en consideración los valores para el negocio de los activos de información y los riesgos desde el punto de vista del negocio de la organización. En el primer punto de decisión (véase la Figura 1) varios factores facilitan la determinación de si la evaluación de alto nivel es adecuada para tratar los riesgos; estos factores pueden incluir los siguientes:

- los objetivos del negocio que se deben alcanzar utilizando diversos activos de información;

- el grado hasta el cual el negocio de la organización depende de cada activo de información, es decir, si las funciones que la organización considera críticas para su supervivencia por la conducta eficaz del negocio dependen de cada uno de los activos, o de la confidencialidad, integridad, disponibilidad, no repudio, responsabilidad, autenticidad y confiabilidad de la información almacenada y procesada en este activo;

- el grado de inversión en cada uno de los activos de información, en términos de desarrollo, mantenimiento o reemplazo del activo;

- los activos de información para los cuales la organización asigna directamente un valor.

Al evaluar estos factores, la decisión se hace más fácil. Si los objetivos de un activo son extremadamente importantes para conducir los negocios de la organización, o si los activos están en alto riesgo, se debería llevar a cabo una segunda repetición, la evaluación detallada del riesgo, para el activo particular de información (o parte de él).

Una regla general a aplicar es: si la falta de seguridad de la información puede dar como resultado consecuencias adversas significativas para una organización, sus procesos del

negocio o sus activos, es necesaria una segunda repetición de la evaluación del riesgo, en un grado más detallado, para identificar los riesgos potenciales.

E.2 EVALUACIÓN DETALLADA DE LOS RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

El proceso de evaluación detallada de los riesgos en la seguridad de la información implica la identificación y evaluación profundas de los activos, la evaluación de las amenazas para tales activos y la evaluación de las vulnerabilidades. Los resultados de estas actividades se utilizan entonces para evaluar los riesgos y luego identificar su tratamiento.

El paso detallado usualmente exige tiempo, esfuerzo y habilidad considerables y por lo tanto puede ser más adecuado para sistemas de información en alto riesgo.

La etapa final de la evaluación detallada de los riesgos en la seguridad de la información es evaluar los riesgos globales, lo cual constituye el enfoque de este anexo.

Las consecuencias se pueden evaluar de varias maneras, incluyendo el uso de medidas cuantitativas, por ejemplo monetarias, y cualitativas (las cuales se pueden basar en el uso de adjetivos tales como moderado o grave) o una combinación de ambas. Para evaluar la probabilidad de ocurrencia de una amenaza, se debería establecer el marco temporal en el cual el activo tendrá valor o necesitará protección. La probabilidad de ocurrencia de una amenaza específica está afectada por los siguientes aspectos:

- Lo atractivo que sea el activo, o el impacto posible aplicable cuando se toma en consideración una amenaza humana deliberada.

- La facilidad de conversión en recompensa de la explotación una vulnerabilidad del activo, aplicable cuando se toma en consideración una amenaza humana deliberada.

- Las capacidades técnicas del agente amenazador, aplicable a amenazas humanas deliberadas.

- La susceptibilidad de la vulnerabilidad a la explotación, aplicable tanto a vulnerabilidades técnicas como no técnicas.

Muchos métodos utilizan tablas y combinan medidas subjetivas y empíricas. Es importante que la organización utilice un método con el cual esté cómoda, en el cual la organización tenga confianza y que produzca resultados repetibles. A continuación se indican algunos ejemplos de técnicas basadas en tablas.

E.2.1 EJEMPLO 1 Matriz con valores predefinidos

En los métodos de evaluación de riesgos de este tipo, los activos físicos reales o propuestos se evalúan en términos de costos de reemplazo o de reconstrucción (es decir, mediciones cuantitativas). Estos costos se convierten después en la misma escala cualitativa a la utilizada para la información (véase más adelante). Los activos de software, reales o propuestos, se evalúan de la misma manera que los activos físicos, con costos de compra o reconstrucción identificados y luego se convierten en la misma escala cualitativa de la utilizada para la información. Además, si se observa que algún software de aplicación tiene sus propios requisitos intrínsecos de confidencialidad o integridad (por

ejemplo si el código fuente es en sí mismo sensible comercialmente), se evalúa de la misma manera que la información.

Los valores para la información se obtienen entrevistando a personas seleccionadas de la gerencia del negocio (los "propietarios de los datos"), quienes pueden hablar con autoridad acerca de los datos, determinar los valores y la sensibilidad de los datos realmente el uso o que se van a almacenar, procesar, o a los que se va tener acceso. Las entrevistas facilitan la evaluación del valor y la sensibilidad de la información en términos de los escenarios más desfavorables cuya ocurrencia razonablemente se podría esperar a partir de consecuencias adversas para el negocio, debidas a divulgación no autorizada, modificación no autorizada, falta de disponibilidad durante diversos períodos de tiempo y destrucción.

La evaluación se logra utilizando directrices para evaluación de la información, las cuales comprenden los siguientes temas:

- Seguridad personal.
- Información personal.
- Obligaciones legales y reglamentarias.
- Cumplimiento de la ley.
- Intereses comerciales y económicos.
- Pérdida financiera/alteración de actividades.
- Orden público.
- Políticas y operaciones del negocio.
- Pérdida del buen nombre.
- Contrato o acuerdo con un cliente.

Las directrices facilitan la identificación de los valores en una escala numérica, por ejemplo la escala de 0 a 4 que se muestra en el ejemplo de matriz, permitiendo así el reconocimiento de valores cuantitativos cuando es posible y lógico, y valores cualitativos cuando no son posibles los valores cuantitativos, por ejemplo cuando se pone en peligro la vida humana.

La siguiente actividad principal es la terminación de pares de concesionarios para cada tipo de amenaza, para cada agrupación de activos con los cuales se relaciona el tipo de amenaza, con el fin de habilitar la evaluación de los niveles de amenazas (probabilidad de ocurrencia) y niveles de vulnerabilidades (facilidad de explotación por parte de las amenazas para causar consecuencias adversas). Cada respuesta a un interrogante suscita un puntaje. Estos puntajes se acumulan a través de una base de conocimientos y se compara con los rangos. Esto identifica los niveles de amenaza en una escala de alto a bajo y los niveles de vulnerabilidad de manera similar, tal como se presenta en el ejemplo de la matriz, diferenciando entre los tipos de consecuencias según sea pertinente. La

información para completar los cuestionarios se debería reunir en entrevistas con personal técnico adecuado y personal de acompañamiento, así como de inspecciones físicas del lugar y revisiones de documentos.

Los valores del activo, y los niveles de amenaza y vulnerabilidad, pertinentes para cada tipo de consecuencias se contrastan en una matriz como la que se indica más adelante con el fin de identificar, para cada combinación, la medida pertinente de riesgo en una escala de 0 a 8. Los valores se ubican en la matriz de manera estructurada. El ejemplo es el siguiente:

Tabla E.1 a)

	Probabilidad de ocurrencia - Amenaza	**Baja**			**Media**			**Alta**		
	Facilidad de explotación	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Valor del activo										

Para cada uno de los valores, las vulnerabilidades pertinentes y sus amenazas correspondientes se toman en consideración. Si existe una vulnerabilidad sin una amenaza correspondiente, o una amenaza sin una vulnerabilidad correspondiente, en el momento no existe riesgo (pero se debe tener cuidado en caso de que esta situación cambie). Ahora, la fila adecuada en la matriz se identifica por el valor del activo, y la columna adecuada se identifica por la probabilidad de ocurrencia de la amenaza y la facilidad que explotación. Por ejemplo, si el activo tiene un valor de **3**, la amenaza es "**alta**" y la vulnerabilidad "**baja**", la medida del riesgo es de **5**. Asumiendo que un activo tiene un valor de 2, por ejemplo para modificación, el nivel de amenaza es "bajo" y la facilidad de explotación es "alta", entonces la medida del riesgo es de 4. El tamaño de la matriz, en términos de la cantidad de categorías de probabilidad de la amenaza, categorías de facilidad de explotación y la cantidad de categorías de valoración de activos, se puede ajustar a las necesidades de la organización. Las columnas y las filas adicionales requerirán de medidas adicionales del riesgo. El valor de este enfoque está en la clasificación de los riesgos que se van a tratar.

Una matriz similar a la que se presenta en la Tabla E.1 a) resulta de la consideración de la probabilidad de un escenarios de incidente, graficado frente al impacto estimado en el negocio. La probabilidad de un escenario de incidente está dada por una amenaza que explota una vulnerabilidad con una probabilidad determinada. La Tabla indica esta probabilidad frente al impacto en el negocio relacionado con el escenario de incidente. El riesgo resultante se mide en una escala de 0 a 8 que se puede evaluar frente a los criterios de aceptación del riesgo. Esta escala de riesgos también se podría trazar para una clasificación más sencilla del riesgo total, por ejemplo así:

- Riesgo bajo: 0-2.
- Riesgo medio: 3 - 5.
- Riesgo alto: 6-8

Tabla E.1 b)

	Probabilidad del escenario de incidente	**Muy baja (muy improbable)**	**Baja (Improbable)**	**Media (Posible)**	**Alta (Probables)**	**Muy alta (Frecuente)**
Impacto en	**Muy baja**					

el negocio	**Baja**					
	Media					
	Alta					
	Muy alta					

E.2.2 EJEMPLO 2 Clasificación de las amenazas mediante las medidas del riesgo

Se puede utilizar una matriz o una tabla para relacionar los factores de consecuencias (valor del activo) y la probabilidad de ocurrencia de la amenaza (teniendo en cuenta los aspectos de vulnerabilidad). El primer paso es evaluar las consecuencias (valor del activo), en una escala predefinida, por ejemplo de 1 hasta 5, de cada uno de los activos amenazados (columna "b" en la tabla). El segundo paso es evaluar la probabilidad de ocurrencia de la amenaza en una escala predefinida, por ejemplo de 1 hasta 5, de cada una de las amenazas (columna "c" en la tabla). El tercer paso es calcular la medida del riesgo multiplicando (b x c). Finalmente, las amenazas se pueden clasificar en orden de sus medidas de riesgo asociadas. Observe que en este ejemplo, 1 se toma como la consecuencia más baja y la probabilidad más baja de ocurrencia.

Tabla E.2

Descriptor de la amenaza (a)	**Consecuencia (valor del activo) (b)**	**Probabilidad de ocurrencia de la amenaza (c)**	**Medida del riesgo (d)**	**Clasificación de la amenaza (e)**
Amenaza A				
Amenaza B				
Amenaza C				
Amenaza D				
Amenaza E				
Amenaza F				

Como se indica en la tabla, este es un procedimiento que permite comparar y clasificar en orden de prioridad diferentes amenazas con diferentes consecuencias y probabilidad de ocurrencia, como se muestra aquí. En algunos casos será necesario asociar valores monetarios a las escalas empíricas utilizadas aquí.

E.2.3 EJEMPLO 3 Evaluación de un valor para la probabilidad y las consecuencias posibles de los riesgos

En este ejemplo, el énfasis se hace en las consecuencias de los incidentes de seguridad de la información (es decir, los escenarios de incidente) y en la determinación de cuáles sistemas deberían tener prioridad. Esto se lleva a cabo evaluando dos valores para cada uno de los activos y riesgos, los cuales en combinación determinarán el puntaje para cada uno de los activos. Cuando los puntajes de todos los activos para el sistema se suman, se determina una medida del riesgo para ese sistema.

Primero, se asigna un valor para cada uno de los activos. Este valor se relaciona con las consecuencias adversas potenciales que se pueden originar si el activo está amenazado. Para cada amenaza aplicable al activo, este valor se asigna a ese activo.

Enseguida se evalúa el valor de la probabilidad. Esta evaluación se hace a partir de una combinación de la probabilidad de ocurrencia de la amenaza y la facilidad de explotación de la vulnerabilidad, véase la Tabla E.3 que expresa la probabilidad de un escenario de incidente.

Tabla E.3

Probabilidad de amenaza	**Baja**			**Media**			**Alta**		
Niveles de vulnerabilidad	L	M	H	L	M	H	L	M	H
Valor de la probabilidad de un escenario de incidente	0	1	2	1	2	3	2	3	4

A continuación, se asigna un puntaje para el activo/la amenaza determinando la intersección del valor del activo y del valor de la probabilidad en la tabla E.4. Los puntajes del activo/la amenaza se totalizan para obtener un puntaje total para ese activo. Esta cifra se puede utilizar para diferenciar entre los activos que forman parte de un sistema.

Tabla E.4

Valor del activo					
Valor de la probabilidad					
0					
1					
2					
3					
4					

El paso final es totalizar todos los puntajes totales de los activos del sistema, obteniendo un puntaje para ese sistema. Este puntaje se puede utilizar para diferenciar entre sistemas y determinar la prioridad que se debería dar a la protección del sistema

En los siguientes ejemplos todos los valores se seleccionan al azar.

Suponga que el sistema S tiene tres valores A1, A2 y A3. Suponga también que existen dos amenazas T1 y T2 que se aplican el sistema S. El valor de A1 es 3, el valor de A2 es 2 y el de 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.3).

El puntaje del activo/la amenaza A1/T1 se puede derivar de la Tabla E.4 como la intersección del valor del activo 3 y el valor de probabilidad 1, es decir 4. De igual modo, para A1/T2, la probabilidad de amenaza es media y la facilidad de explotación de la vulnerabilidad es alta, se tiene un puntaje para A1/T2 de 6.

Ahora, se puede calcular el puntaje total de los activos A1T, es decir 10. El puntaje total del activo se puede calcular para cada uno de los activos y amenazas aplicables. El puntaje del sistema total se calcula sumando A1T + A2T + A3T para obtener ST.

Se pueden comparar sistemas diferentes para establecer prioridades y diferenciar activos dentro de un sistema.

Los ejemplos anteriores se presentan en términos de sistemas de información, sin embargo, un enfoque similar se puede aplicar a los procesos del negocio.

ANEXO F
(Informativo)

RESTRICCIONES PARA LA REDUCCIÓN DE RIESGOS

Al considerar las restricciones para la reducción de riesgos se deberían tener en cuenta las siguientes:

Restricciones de tiempo:

Pueden existir muchos tipos de restricción del tiempo. Por ejemplo, se deberían implementar controles dentro de un periodo de tiempo aceptable para los directores de la organización. Otro tipo de restricción del tiempo es si un control se puede implementar durante la vida activa de la información o del sistema. Un tercer tipo puede ser el periodo de tiempo que los directores de la organización deciden que es aceptable para estar expuestos a un riesgo particular.

Restricciones financieras:

Los controles no deberían ser más costosos en su implementación o mantenimiento que el valor de los riesgos que van a proteger, excepto cuando la conformidad es obligatoria (por ejemplo con la legislación). Se deberían hacer todos los esfuerzos para no exceder los presupuestos asignados y lograr la ventaja financiera a través del uso de los controles. Sin embargo, en algunos casos, puede no ser posible alcanzar la seguridad que se busca ni el nivel de aceptación del riesgo debido a las restricciones de presupuesto. Por lo tanto, esta se convierte en una decisión de los directores de la organización para resolver esta situación.

Se recomienda tener mucho cuidado si el presupuesto reduce la cantidad o la calidad de los controles que se van a implementar dado que esto puede llevar a la retención implícita de un riesgo mayor a la planificada. El presupuesto establecido para los controles se debería utilizar únicamente como un factor limitante con cuidado considerable.

Restricciones técnicas:

Los problemas técnicos, como la compatibilidad de programas o hardware, se pueden evitar fácilmente si se tienen en cuenta durante la selección de los controles. Además, la implementación retrospectiva de controles para un proceso o un sistema existentes a menudo está obstaculizada por restricciones técnicas. Estas dificultades pueden desplazar la balanza de controles hacia aspectos físicos y de procedimiento de la seguridad. Puede ser necesario revisar el programa de seguridad de la información con el fin de lograr los objetivos de seguridad. Esto puede suceder cuando los controles no satisfacen los resultados esperados en la reducción de riesgos sin disminuir la productividad.

Restricciones operativas:

Las restricciones operativas, como por ejemplo la necesidad de trabajar 24 horas durante los siete días de la semana y aún así realizar copia de soporte, pueden dar como

resultado una implementación costosa y compleja de los controles, a menos que ellos se construyan en el diseño desde el principio.

Restricciones culturales:

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

Restricciones éticas:

Las restricciones éticas pueden tener implicaciones importantes en los controles dado que la ética cambia con base en las normas sociales. Esto puede evitar la implementación de controles tales como la exploración del correo electrónico en algunos países. La privacidad de la información también se puede hacer dependiente de la ética de la región o del gobierno. Esto puede ser de más interés en algunos sectores industriales que otros, por ejemplo, gubernamental y de salud.

Restricciones ambientales:

Los factores ambientales pueden influir en la selección de los controles tales como la disponibilidad del espacio, las condiciones climáticas extremas, la geografía urbana y natural del entorno. Por ejemplo las pruebas para terremotos pueden ser necesarias en algunos países pero no en otros.

Restricciones legales:

Factores legales tales como la protección de datos personales o las disposiciones de códigos criminales para el procesamiento de la información podrían afectar la selección de controles. El cumplimiento legal y reglamentario puede determinar algunos tipos de controles, que incluyen la protección de datos y las auditorías financieras; también pueden evitar el uso de algunos controles, por ejemplo la codificación. Otras leyes y reglamentos también podrían afectar la selección de los controles, por ejemplo la legislación sobre relaciones laborales, del departamento de bomberos, de salud y seguridad, regulaciones del sector económico, etc.

Facilidad en el uso:

Una interfaz entre tecnología - humano deficiente resultará en un error humano y puede hacer que el control sea inútil. Los controles se deberían seleccionar de modo que brinden facilidad óptima en el uso al tiempo que alcanzan un nivel aceptable de riesgo residual para el negocio. Los controles que son difíciles de utilizar tendrán impacto en su eficacia, ya que los usuarios pueden intentar burlarlos o ignorarlos en la medida de lo posible. Los controles de acceso complejo dentro de una organización podrían alentar a los usuarios a encontrar métodos de acceso alternos, no autorizados.

Restricciones de personal:

La disponibilidad y el costo de salario de habilidades especializadas para implementar los controles, y la capacidad para trasladar al personal entre los lugares en condiciones de operación adversa, se deberían tomar en consideración. La experiencia puede no estar fácilmente disponible para implementar controles planificados o puede sobrepasar los costos de la organización. Otros aspectos tales como la tendencia de parte del personal a discriminar a otros miembros del personal que no se han seleccionado para la seguridad pueden tener implicaciones importantes para las políticas y prácticas de seguridad. De igual modo, la necesidad de contratar a las personas correctas para el trabajo y hallar a las personas correctas, puede resultar en la contratación antes de finalizar la clasificación de la seguridad. El requisito para completar la clasificación de seguridad antes de la contratación es la práctica normal y más segura.

Restricciones para integrar controles nuevos y existentes:

La integración de controles nuevos en la infraestructura existente y las interdependencias entre los controles a menudo se pasan por alto. Los controles nuevos pueden no ser implementados fácilmente si hay incongruencia o incompatibilidad con los controles existentes. Por ejemplo, un plan para utilizar fichas geométricas para el control del acceso físico puede causar conflictos con un sistema existente basado en teclados numéricos (PIN-pad) para el control del acceso. El costo del cambio de los controles existentes por los controles planificados debería incluir elementos que se van a adicionar al costo total del tratamiento del riesgo. Puede no ser posible implementar un control seleccionado debido a la interferencia con controles actuales.

BIBLIOGRAFÍA

[1] ISO/IEC Guide 73:2002, *Risk Management. Vocabulary. Guidelines for Use in Standards.*

[2] ISO/IEC 16085:2006, *Systems and Software Engineering. Life Cycle Process. Risk Management.*

[3] AS/NZS 4360:2004, *Risk Management*.

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

[5] NIST Special Publication 800-30, *Risk management Guide for Information Technology Systems, recommendations of the National Institute of Standards and Technology.*

PROYECTO DE
NORMA TÉCNICA COLOMBIANA NTC-ISO 27005 DE 174/08

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Information Security Risk Management. Geneva: ISO, 2008, 65 p (ISO/IEC FDIS 27005:2008 (E)).

PREPARADO POR: _____
FERNANDO MORENO

rrc.