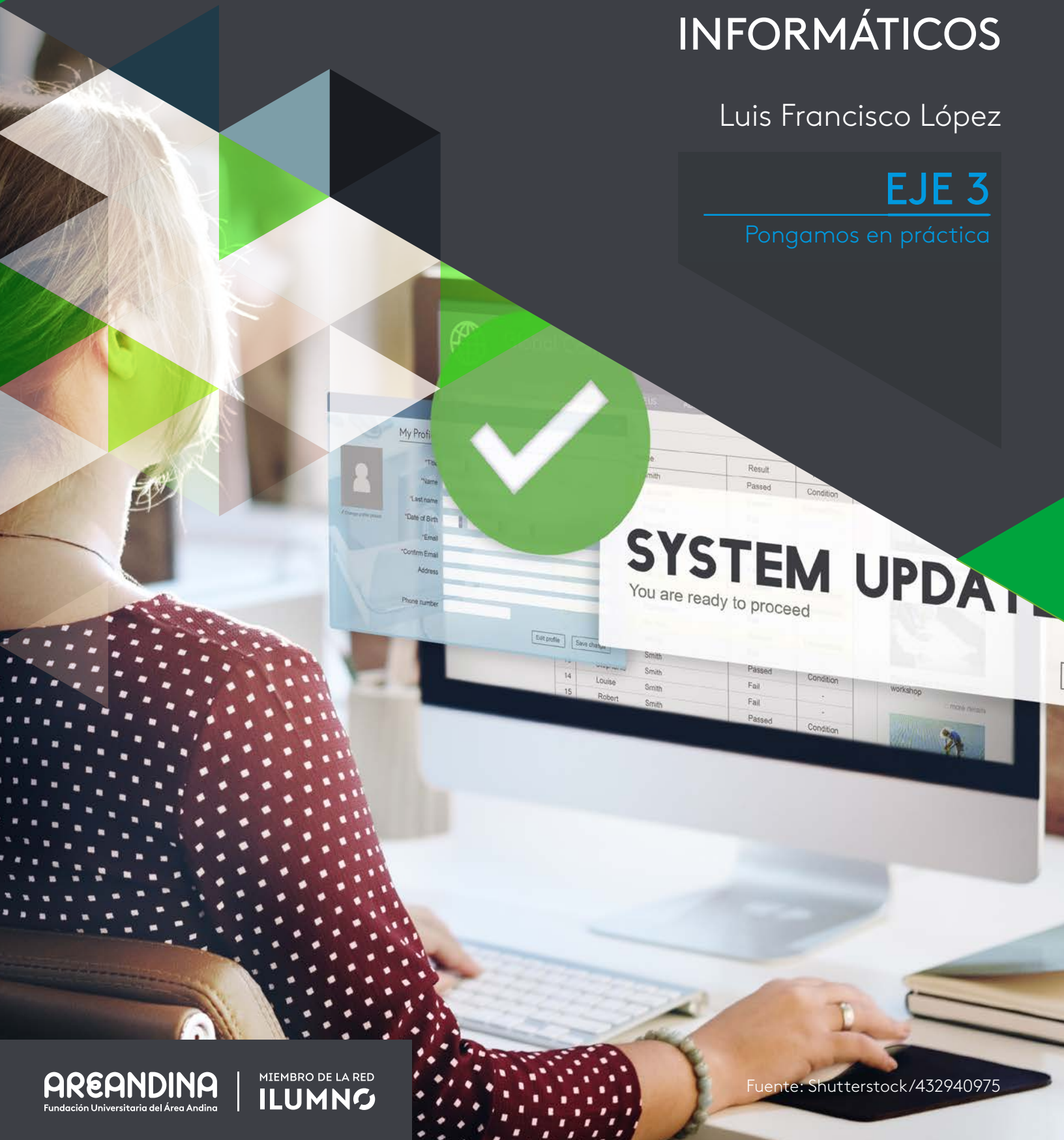
ANÁLISIS DE RIESGOS INFORMÁTICOS

Luis Francisco López

EJE 3

Pongamos en práctica



AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

Fuente: Shutterstock/432940975

ÍNDICE

INTRODUCCIÓN

¿Cómo se diseña un sistema de gestión de riesgos informáticos SGSI que conjugue las normas técnicas con los modelos existentes para la industria?

El contexto particular que define cada uno de los elementos que hacen parte de una organización genera un ambiente único y a veces irrepetible en el entorno de las organizaciones, así, prácticas como el liderazgo horizontal, sumadas a estrategias para que los trabajadores se sientan parte de una organización pueden impactar de forma significativa en la mejora del rendimiento de los procesos que se desarrollan a su interior. Sin embargo, situaciones como la que describo a continuación pueden implicar un riesgo para la seguridad de la información que nadie desde la dirección o el componente de tecnologías de la información y las comunicaciones pudo tener en cuenta.

La organización Protejo su Información cuenta con un equipo de trabajo profesional y orienta su misión a administrar y respaldar la información de sus clientes con garantía de confidencialidad, integridad y disponibilidad de la información a través de una red VPN en cualquier momento y en cualquier sitio, según los permisos de acceso del usuario autenticado; por la forma de gestionar los procesos, y con el propósito de no contratar personal adicional, un auxiliar administrativo que está asignado a múltiples dependencias es el encargado de atender las comunicaciones y solicitudes telefónicas en el horario en que la persona encargada de la recepción se encuentra en su período de almuerzo o descanso en cada jornada; para no perder un "cliente" potencial, la persona encargada de la recepción le entrega su sesión en la red corporativa abierta para que pueda dejar el registro de la llamada y agregue la información nueva a la base de datos de posibles clientes.

Las credenciales de la persona encargada de la recepción cuentan con autorización para acceder a todas las bases de datos de la organización, clientes, proveedores, cuentas, portafolio de servicios, correspondencia, entre otras. ¿Existe algún riesgo asociado a la política que la empresa implementó para atender esta situación?

Una situación como la descrita expone apenas uno de los riesgos que es posible identificar en el entorno de la administración y gestión de la información en una organización. De este modo, cualquier sistema que se oriente al análisis y por supuesto mitigación del riesgo en la seguridad de la información debe atender, entre otras, situaciones en relación con el uso de las credenciales de acceso al sistema y los niveles de autorización que se asocian a cada usuario, grupo de usuarios o cuentas individuales.

Administración basada en procesos

Con el desarrollo de un marco de normas y estándares para facilitar la gestión al interior de las organizaciones, la ISO (International Organization for Standarization) por sus siglas en inglés, orienta a las organizaciones y empresas que incorporan los estándares que se expiden al incorporar la administración basada en procesos para facilitar el logro de los objetivos y un adecuado y oportuno seguimiento de su desarrollo (ISO 9001).

Se define entonces un proceso como un conjunto de actividades que se encuentran relacionadas entre sí y que se desarrollan de forma ordenada para el logro de un objetivo, en este caso el objetivo es transformar unos insumos que ingresan al proceso en un producto o resultado en su salida. En este mismo orden de ideas, el resultado de un proceso se puede constituir en uno de los insumos de entrada del siguiente proceso, así se puede garantizar un control estricto en todas las etapas.

Los elementos que según la norma incorpora un proceso se agrupan en:

- Elementos de entrada y salida: según la misión y objetivos de la organización se pueden identificar elementos tangibles o intangibles, además en la salida pueden presentarse desviaciones, por ejemplo, en un SGSI una salida inesperada de un proceso puede generar una reducción del consumo de papel en la organización.

- Clientes y terceros interesados: las condiciones del resultado se deben ajustar a las necesidades o requerimientos que ellos plantean, es posible que el cliente sea interno, así como otra dependencia de la organización que recibe el resultado de un proceso para desarrollar una nueva transformación.

- Sistemas de control y/o medición: la administración orientada a procesos busca que al interior de la organización cada uno de los procesos que se incorporan cuente con mecanismos de control que permitan ajustar los resultados en función de los objetivos y controles.

Así, la norma ISO 27005:2018 propone un conjunto de lineamientos que se deben incorporar a un SGSI para que se oriente a la gestión del riesgo de la seguridad de la información. El estándar se puede aplicar, independiente de su tamaño, a cualquier organización que administre información a través de medios digitales y no tenga una metodología específica, deja a potestad de las directivas definir cómo se va a implementar según el alcance del SGSI, el objetivo de la compañía y el sector en que se desempeña. Desde esta perspectiva, el análisis del riesgo y los procedimientos para su desarrollo recaen sobre la misma organización, así es posible que se haga de forma inicial un análisis de vulnerabilidades en función del riesgo externo y de forma seguida se efectúe un análisis de las amenazas asociadas a factores de exposición internos, por ejemplo.

Metodologías y modelos para el análisis y gestión del riesgo

Como se describe a lo largo del curso, los estándares relacionados en el conjunto de normas ISO 27000 no definen una metodología o procedimientos en particular para elaborar un sistema de gestión de la seguridad de la información que incorpore la gestión del riesgo, sin embargo, los lineamientos que propone delimitan de forma

precisa los elementos y alcance que debe incorporar el sistema para que se pueda afirmar que incorpora su análisis y gestión.

- Tratamiento del riesgo: se define entonces el riesgo "como una amenaza que explota la vulnerabilidad de un activo pudiendo causar daños" (ISO 27005, 2018). Es claro entonces que para estar expuestos al riesgo se hace implícito el uso de la infraestructura de tecnologías y comunicaciones de la organización.

- Gestión del riesgo: se recomienda aplicar el enfoque de procesos para su gestión y definir uno que se ajuste a las condiciones particulares de la organización, que sea estructurado, sistemático, riguroso y que produzca como salida un plan de la organización para tratar los riesgos. Este plan debe incorporar algunos indicadores clave que hagan evidente si la compañía se encuentra expuesta a niveles de riesgo más altos que los previstos en el plan.

- Evaluación del plan de tratamiento del riesgo: como parte del plan se debe incorporar la posibilidad de hacer una evaluación continua de cada uno de los procesos que se incluyen como parte del plan de tratamiento de riesgos. El sistema debe ser flexible en tanto permita su ajuste a elementos sobrevinientes, como el caso de un nuevo virus o amenaza tipo *ransomware* que aproveche brechas de seguridad desconocidas hasta el momento en los sistemas operativos o aplicaciones que se ejecutan en la plataforma.

- Identificar los riesgos: la norma ISO 27005:2018 asocia el término incertidumbre a la presencia de un riesgo; en este sentido, se asocia el riesgo a algún grado de incertidumbre, es decir si tengo una certeza absoluta de las consecuencias que puede tener una amenaza que se materializa solo se habla de riesgo por la posibilidad que se presente más no por sus consecuencias, porque estas ya se tienen en cuenta dentro del plan de tratamiento del riesgo.

Incertidumbre
Desconocimiento de alguna situación o estado posible. En gestión de riesgos, el riesgo implica la certeza de que algún resultado adverso se pueda presentar, la incertidumbre puede tener efectos positivos o negativos sobre los resultados de la organización.

La incertidumbre puede medirse según el efecto que causa el riesgo sobre los resultados del negocio o sobre los elementos que componen el sistema de gestión de la información. De esta manera, si nuestra compañía vende productos o servicios tasados en dólares el riesgo que existe está asociado a la variación del precio del dólar en el mercado colombiano y la incertidumbre es qué tanto sube o baja. Es claro que situaciones como la que describo pueden afectar de forma significativa el valor de los activos de nuestra organización, así la recomendación para empresas de tamaño pequeño o mediano es evitar o minimizar este tipo de riesgos.

- Causas y efectos de los riesgos: una situación que con frecuencia se presenta es la confusión que los encargados del diseño del sistema pueden tener al identificar el riesgo o los riesgos existentes para un activo en particular, por ejemplo cuando el equipo de seguridad decide reemplazar el *software* antivirus en distintas sucursales pero como es frecuente no todos los computadores cuentan con la misma plataforma de *hardware* ni en las versiones y actualizaciones de sistemas operativos se pueden presentar situaciones como las que describo.

  - El reemplazo o instalación del antivirus se puede considerar un riesgo? No, es una disposición de la organización para mitigar el impacto de una amenaza y para reducir la exposición a riesgos.

  - ¿Si la plataforma de *hardware* o la versión del sistema operativo de la organización no admite el reemplazo del antivirus, puede ser considerado un riesgo? Por supuesto, si la compañía toma la decisión de comprar un nuevo antivirus y hacer la actualización de todos los computadores, debió someter a una evaluación el anterior *software* y encontrar vulnerabilidades que implican el cambio. Entonces, si en algún computador no se puede hacer la instalación este equipo quedaría vulnerable y con mayor exposición a riesgos.

  - ¿Existe algún riesgo adicional a la imposibilidad de instalar el nuevo antivirus? Hay una incertidumbre que solo puede ser asumida como riesgo una vez se conozca el informe de las razones por las cuales no fue posible la instalación.

Riesgos en la infraestructura de TI

Figura 1. Sistemas operativos
Fuente: Shutterstock/781714462

Como se explica en el desarrollo del curso, las debilidades de un activo o sistema trae implícito un riesgo, por tal razón identificar elementos clave en el sistema de gestión de la seguridad de la información es una tarea fundamental en el análisis y gestión de riesgos, a continuación, enumero algunos riesgos que se pueden identificar en una plataforma de TI:

- Aplicaciones de *software* desactualizadas, sin licencias vigentes y sin parches de seguridad hacen que el sistema sea vulnerable.

- Sistemas operativos que no cuentan con las últimas actualizaciones instaladas o en condiciones de fin de ciclo de vida, por ejemplo, para Windows XP o Server 2003 la empresa Microsoft ya no expide actualizaciones, por tanto, tener sistemas de este tipo en nuestra plataforma implica un riesgo.

- Aplicaciones propias con desarrollo inseguro: cuando el departamento de desarrollo de la organización crea aplicaciones para el uso interno y no atiende recomendaciones en relación con el uso de memoria, apuntadores y otras condiciones de seguridad, pueden fallar o dejar recursos de memoria libres que constituyen un riesgo porque a través de ellos se puede materializar una amenaza.

- Tecnología desactualizada: por ejemplo, en la red corporativa el uso de *hubs* o *switches* de capa dos que no permiten implementar ninguna política de seguridad hacen que la plataforma sea vulnerable.

- Servicios de terceros no seguros: la organización para acceder a redes públicas contrata con un ISP un servicio de internet banda ancha sobre un canal de cobre, se trata de un enlace de red punto a punto sobre el que la organización no cuenta con un control para cifrar y proteger las comunicaciones, así estamos asumiendo un riesgo.

Las anteriores son algunas situaciones asociadas a la plataforma de tecnologías de la información y las comunicaciones de la organización que pueden implicar algún tipo de riesgo.

Lectura complementaria

Para entrar en detalle respecto a los riesgos y su tratamiento le recomiendo hacer la lectura de los apéndices I y J del texto disponible en la página principal del eje:

Norma NIST 800-30 (pp. i1 a j2)

National Institute of Standards and Technology

Antes de iniciar el análisis de los sistemas más usados en el mundo para el análisis y gestión de los riesgos informáticos, es necesario que ustedes, apreciados estudiantes, recuerden que no es obligatorio que en el diseño de un sistema nos ajustemos cien por ciento a los lineamientos que se definan en alguno de ellos, algunas organizaciones toman partes de un modelo y las incorporan junto con partes de otro modelo para darle más "robustez", situación que no recomiendo. Sin embargo, sea cual sea el modelo que se implemente para el análisis y gestión del riesgo informático, la norma ISO 31000:2018 define los principios básicos a los que se debe ajustar un proceso para la gestión de riesgos informáticos.

Instrucción

Se sugiere revisar el podcast disponible en la página principal del eje.

Principios para la gestión de riesgos

Los principios básicos que la norma contempla en un sistema de gestión de riesgos a saber:

- Crea y protege el valor: apoya el logro de los objetivos de la organización y de otra parte emite un valor agregado a los procesos, por ejemplo, reduce el impacto ambiental de la organización al minimizar el consumo de papel.
- Hace parte de todos los procesos: a pesar de que el término suene inadecuado se debe convertir en una política de la organización.
- Hace parte del proceso para la toma de decisiones: la toma de decisiones en la dirección de la organización debe estar alineada con el análisis y gestión del riesgo.
- Se debe usar para tratar la incertidumbre: en el plan de gestión de riesgo se deben plantear escenarios para atender escenarios o aspectos inciertos, su origen y las posibles consecuencias.
- Estructurado, sistemático y oportuno: es necesario que el plan se articule a partir de un proceso estratégico, que atienda las condiciones particulares de la compañía, y se adelante en los momentos indicados, ¿qué sentido puede tener un plan para la gestión del riesgo informático que se implementa luego que la organización sea víctima de un ataque en el que perdió una gran cantidad de información?
- Es necesario contar con información precisa y adecuada: el análisis y gestión del riesgo informático se debe planear y ejecutar a partir de información pertinente y adecuada al contexto dentro del cual se incorpora con datos recientes.
- Debe estar ajustado al entorno en el cual se implementa: asumir políticas o prácticas que se recomiendan en grandes corporaciones puede impactar de forma negativa e inclusive exponer a mayores riesgos a una pequeña compañía que la incorpore.
- Debe tener en cuenta los factores humanos y culturales que afectan la organización: el análisis y gestión del riesgo informático al interior de la organización exige atender las condiciones particulares de las personas que trabajan en ella o los clientes, por ejemplo, el nivel de formación de los trabajadores es un factor clave en el diseño del sistema.
- El sistema debe ser dinámico, sensible al cambio e iterativo: el análisis y gestión del riesgo deben atender los cambios que se presentan al interior de la organización, sus distintos contextos, los riesgos emergentes y los que pueden haber desaparecido.

- Debe estar orientado a la mejora continua: un sistema escalable y flexible debe atender y ser una oportunidad para la mejora continua al interior de la organización.

Recuerden entonces, apreciados estudiantes, que el análisis y diseño de un sistema de gestión del riesgo informático debe atender los principios que se mencionan.

Instrucción

Es momento de consultar la infografía en la página principal del eje.

A continuación, se explican los métodos de análisis y gestión de riesgos informáticos de uso más extendido en el mundo; no entramos en detalle sobre el método cualitativo NIST 800-30 porque ya se abordó en el desarrollo del módulo sociocrítico.

Instrucción

Le invitamos a la página principal del eje para realizar el control de lectura.

Herramientas para el análisis y gestión de riesgos

Metodología Magerit

Es el modelo de uso obligatorio para todas las entidades de la administración pública en España. Su nombre es el acrónimo de las palabras "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", está compuesta por tres volúmenes, a saber:

- Volumen I: método que explica la metodología en detalle.
- Volumen II: catálogo de elementos, incluye los elementos de referencia que se deben tener en cuenta en el desarrollo de la metodología.
- Volumen III: guía de técnicas, se constituye en el elemento que complementa la descripción de la metodología, reúne las tablas, matrices y demás elementos que se pueden usar en el análisis de riesgos.

El diagrama que se incluye a continuación es una interpretación de la metodología de acuerdo a su estructura.

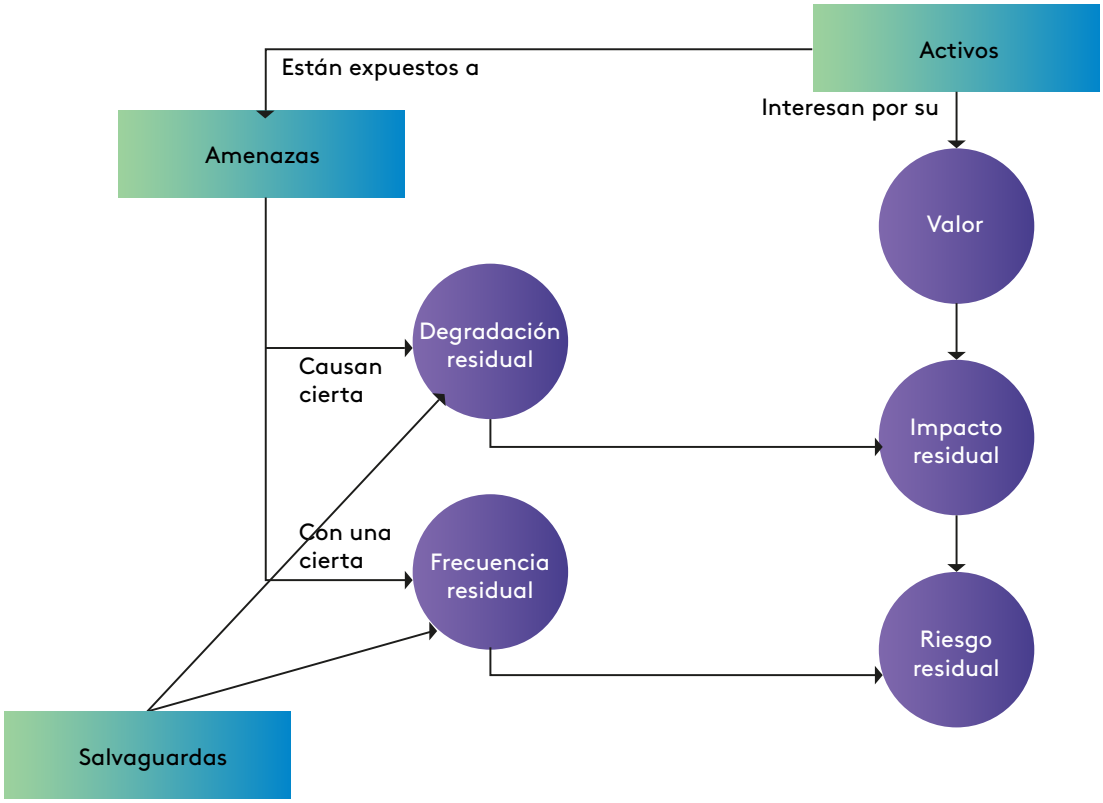


Figura 2. Metodología Magerit
Fuente: Matalobos (2009)

Las características de la metodología Magerit se describen abajo:

a. Implica que los responsables del sistema de información se hagan conscientes de que en todo momento se encuentran expuestos a riesgos.
b. Pone a disposición de los responsables del sistema un método para su análisis.
c. Su implementación ayuda a descubrir riesgos e implementar procedimientos adecuados para mitigar o evitar que se materialicen y provoquen daños o pérdidas para la organización.
d. Prepara a la organización para acreditar su sistema de gestión de la seguridad de la información y para responder a distintos tipos y niveles de auditoría.

La metodología se desarrolla en tres fases, a saber:

1. Análisis de los riesgos: a partir de la información que se suministra en el volumen uno, se analizan los riesgos a los que se encuentran expuestos los activos; para este análisis se debe trazar la información con el catálogo de elementos que se incluyen en el volumen dos.
2. Caracterización de los activos: esta etapa incluye tres elementos:
   - Según el catálogo que se menciona en el volumen dos se describen y caracterizan las amenazas.
   - Se deben definir y caracterizar las medidas de mitigación o salvaguardas.
   - Como resultado se elabora una matriz con la estimación del estado del riesgo.
3. Se gestionan los riesgos de acuerdo a los resultados de los dos pasos anteriores.

Como ventajas del uso de esta metodología se destacan:

- Por su alcance, todo el ámbito de la organización se considera robusto puesto que aplica la gestión de riesgos a cada uno de los procesos que se desarrollan al interior de la organización.
- Su catálogo de recursos es muy amplio y completo, de este modo permite cubrir un amplio abanico de posibilidades, tanto en el listado y categorías de amenazas, debilidades y activos.
- Incluye elementos de carácter cuantitativo y cualitativo.
- Es de uso público y no se requiere autorización para usarlo e implementarlo en una organización.

Dentro de sus desventajas se encuentran:

- Busca cuantificar las amenazas y los riesgos en términos económicos, así se hace muy difícil estimar en esos términos el impacto de ciertos riesgos o cuantificar, por ejemplo, el valor de los recursos humanos o clientes.

- Cuenta con poca o nula orientación para el análisis de políticas o del gobierno corporativo.

Lectura complementaria

Le recomiendo hacer un análisis en detalle del modelo con ayuda de la lectura disponible en la página principal del eje:

Gestión de Riesgos. Magerit (pp. 16-20)

tiThink Consultoría

Modelo Cramm

Este modelo se desarrolla a partir de una iniciativa de la Agencia Central de Comunicación y Telecomunicaciones del Gobierno británico, CCTA por sus siglas en inglés; su primera publicación se hace en el año 1985 y en la actualidad se encuentra en su versión 5.1 expedida en 2005. Su nombre es un acrónimo de Risk Análisis and Management Method: método para el análisis y administración del riesgo.

Es el método que las autoridades del Gobierno británico exigen a todas las entidades gubernamentales para la gestión de riesgos de la seguridad en la información. Una de las ventajas del uso del modelo Cramm radica en la posibilidad de emitir los informes en términos numéricos (cuantitativos) o de calificación de características (cualitativo), por esta razón se le considera un método mixto.

Se desarrolla en tres etapas que se describen a continuación:

1. Definir el alcance del sistema: incluye los objetivos y la caracterización del sistema; en esta caracterización se deben incluir los activos (en todas las categorías disponibles) y asignar un valor a la información que se administra bajo el sistema en clave de su impacto para cumplir los objetivos de la organización. Se deben cumplir las siguientes tareas:

- Identificar y delimitar el contexto del sistema y su alcance.

- Asignar un valor a la información que se administra en el sistema, se recomienda hacer este estudio a través de métodos cualitativos como entrevistas a los usuarios. Los activos físicos, por ejemplo, *hardware* y *software* se valoran en términos del costo comercial o su valor de reemplazo, es decir: cuál es su valor en el mercado si se hace necesario cambiarlo por otro. Los activos intangibles como la información se valoran en función del impacto que su pérdida, modificación, divulgación o uso indebido que pueda causar a la organización.

- Elaborar una matriz que incluya los activos de que dispone el sistema en su valor monetario, su rol en el sistema.

- Construir una matriz que incluya los componentes de *software* de propiedad de la compañía o licenciado por terceros que hacen parte del sistema, se debe además describir su rol, procedencia e importancia.

2. Análisis y evaluación de los riesgos, este análisis debe incluir las amenazas a las que se encuentran expuestos los activos y señalar las vulnerabilidades a través de las cuales estas se pueden materializar y calcular el riesgo que puede implicar que una de ellas lo haga.

Instrucción

Lo invitamos a la página principal del eje para revisar el video con preguntas.

En esta etapa se deben elaborar los siguientes informes:

- Identificar y asignar un valor sobre una escala a las amenazas que pueden afectar el sistema.

- Asignar un valor a las vulnerabilidades del sistema en función de las amenazas que las pueden afectar.

- Elaborar una matriz de medida del riesgo a partir de la relación entre la amenaza y la vulnerabilidad.

La escala de valoración que emite Cramm está en un rango de uno (1.0) a siete (7.0), donde uno representa un nivel de baja exigencia de seguridad y siete representa el máximo nivel de seguridad esperado. De esta forma, los resultados que se obtienen se triangulan con la base de datos de medidas de contención que incluye el modelo. Estas medidas cuentan con un valor de referencia predefinido de modo que se pueda aplicar una medida para un valor estimado de siete (7.0) si el valor obtenido en el análisis de riesgos obtiene ese mismo valor. Este diseño facilita seleccionar las medidas adecuadas según el nivel de riesgo.

3. El modelo incluye un listado de 3 000 medidas de seguridad o contención que se pueden aplicar en la implementación del modelo para mitigar el impacto de una amenaza y obtener lo que se conoce como riesgo residual. El *software* del sistema aplica una medida de contención o contra medida entre una de las setenta categorías en que se agrupan las 3 000 medidas con base en la calificación que se obtiene en la etapa anterior.

Riesgo residual
El resultado de aplicar un análisis de riesgos e implementar medidas de control o mitigación sobre un activo y sus amenazas se conoce bajo esta categoría.

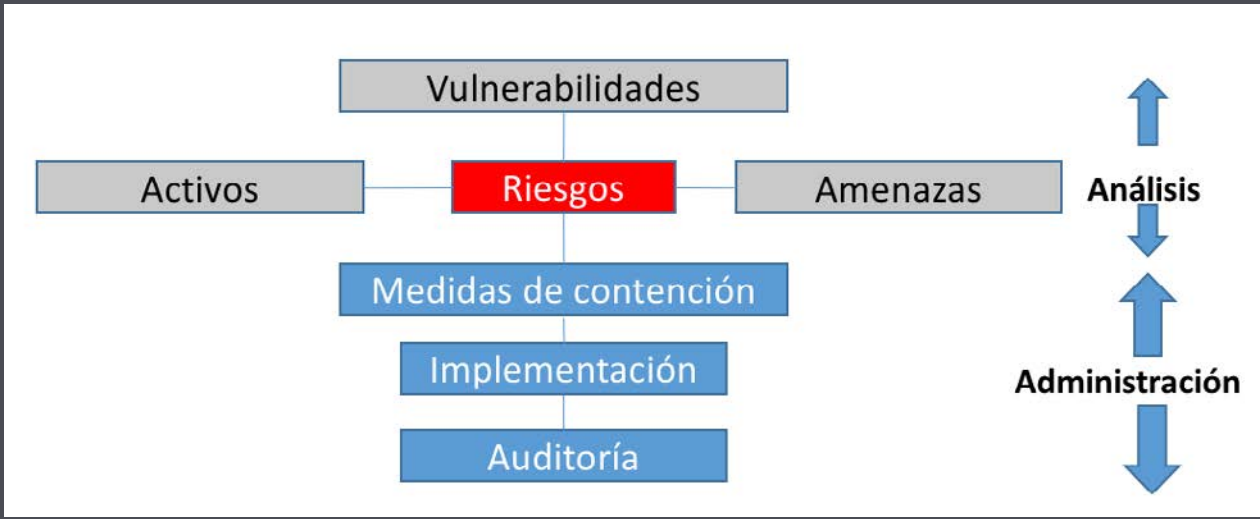


Figura 3. Modelo Cramm
Fuente: propia

De Cramm se destaca que cuenta con un programa o *software* que se orienta a cumplir de forma específica cada una de las etapas que integra el modelo, y permite que el usuario seleccione de entre los siguientes elementos una base de datos que incluye más de 400 activos, un línea de base que incluye más de 25 impactos posibles de las amenazas sobre los activos, 38 amenazas específicas de las cuales se pueden obtener varias subcategorías, una escala con siete niveles de medición del riesgo y una amplia base de datos que incluye más de tres mil quinientas (3 500) medidas de contención, mitigación o salvaguardas.

El *software* que incluye Cramm es de carácter gratuito para empresas del sector público del Reino Unido y se distribuye en el sector comercial con un valor promedio en el mercado para soluciones de este tipo, en especial en el área de auditoría.

La documentación que debe presentar una organización que incorpora el modelo Cramm para la gestión de riesgos informáticos es la siguiente:

1. Documento de inicio del proceso, incluye la caracterización del sistema.

2. Documento en el que se hace el análisis de los riesgos a partir de su relación con las amenazas.

3. Informe en el que especifican las medidas de contención que se implementan como parte del modelo en función de los resultados del análisis y evaluación obtenidos en el segundo documento.

4. Diseño de un plan de implementación del sistema al interior de la organización.

La figura representa el modelo Cramm y sus etapas:

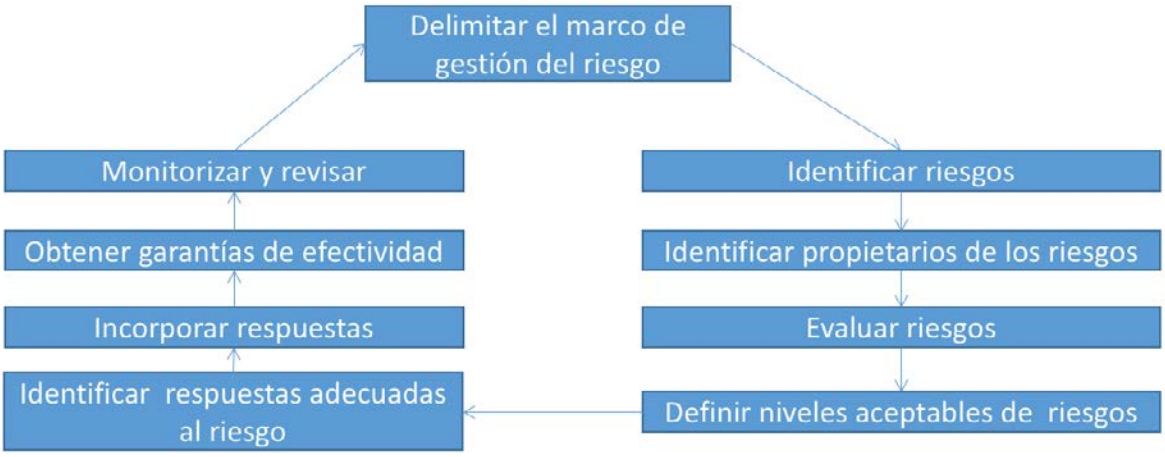


Figura 4. Etapas de Cramm
Fuente: propia

Modelo Octave

Su nombre es el acrónimo de Operationally Critical Threat, Asset and Vulnerability Evaluation. Este modelo se desarrolló por el Instituto de Ingeniería de Software, (SEI) por sus siglas en inglés, de la Universidad de Carnegie Mellon, ubicada en la ciudad de Pittsburgh, estado de Pensilvania en los Estados Unidos; a diferencia de los demás modelos, Octave no propone una serie de pasos a desarrollar, establece un núcleo común que reúne tres elementos: principios, atributos y resultados y, con base en estos elementos, propone el desarrollo de distintas metodologías.

Así, en tanto se apliquen los principios básicos del modelo se puede afirmar que el modelo se ajusta a Octave, sin embargo, el SEI expide tres modelos básicos de Octave:

- Octave. Se trata del método básico que se define como principal, es el primer desarrollo y su diseño se ajusta a organizaciones que administran y gestionan muy elevados volúmenes de información.

- Octave-s. Es un modelo simplificado que se recomienda para compañías que tienen un reducido volumen de información y que en general no administran o gestionan información de terceras partes.

- Octave Allegro. Es un enfoque de la metodología que se orienta al análisis y gestión de riesgos en función de los activos de información.

Para implementar Octave una organización debe cumplir con unos principios básicos que se enuncian a continuación:

- Metodología autodirigida.
- Se debe ajustar a las necesidades de la organización.
- Se debe caracterizar y delimitar el proceso de implementación del método.
- Se debe garantizar su continuidad.
- Debe contar con una proyección a largo plazo.
- Se debe enfocar en reducir al mínimo la cantidad de riesgos críticos.
- La gestión de todo el proceso debe ser integrada.
- La comunicación entre las partes que integran el proceso de desarrollo del modelo debe ser abierta.
- Se debe atender el proceso desde una perspectiva global y no particular.
- Es necesario definir y poner en contexto el equipo de trabajo, sus integrantes, capacidades y responsabilidades.

Según el modelo de Octave que se implementa se hace necesario atender un grupo de fases que incorporan procesos de obligatorio cumplimiento:

Modelo Octave

Fase 1. Visión de la organización, en esta fase se hace necesario:

- Establecer qué conocimiento tiene la alta dirección del SGSI y de los riesgos informáticos inherentes a sus actividades.

- Poner en evidencia cómo se visualizan desde la dirección las áreas operativas de la organización.

- Elaborar la caracterización de las competencias y habilidades con que cuenta el personal de las áreas de tecnologías de la información y los

demás empleados que operan la plataforma tecnológica.

- Levantar un informe de los tipos y características de las amenazas que pueden afectar a la organización.

Fase 2. Visión de la plataforma tecnológica de la organización, en la que se destacan estos aspectos:

- Listar, definir y caracterizar los elementos críticos de la plataforma tecnológica.
- Hacer una evaluación de sus condiciones.

Fase 3

- Análisis de los riesgos.
- Diseño de la estrategia de protección de la información.

Modelo Octave-s

Fase 1. Visión de la organización

- Hacer una caracterización con la información básica de la organización.
- Elaborar un listado con los tipos de amenazas a las que se encuentra expuesta la organización y su plataforma tecnológica.

Fase 2. Visión tecnológica

- Hacer un informe detallado de la plataforma tecnológica en clave del papel que los activos críticos desempeñan en ella y su interrelación con los demás elementos.

Fase 3. Estrategia y desarrollo del plan

- Elaborar un análisis en detalle de los riesgos asociados a las debilidades apuntadas sobre la plataforma tecnológica y los activos críticos.
- Trazar la propuesta para proteger los activos y los planes de contención o mitigación del riesgo.

Como se puede observar, el modelo Octave-s se puede ajustar de manera precisa a pequeñas organizaciones que no pueden desplegar un amplio equipo de expertos para el diseño y toma de decisiones en relación con el modelo de gestión de riesgos y en lo general, la responsabilidad recae sobre el ingeniero o administrador de la plataforma y el responsable de la dirección de la organización.

Instrucción

Realice la demostración de roles disponible en la página principal del eje.

Modelo Octave Allegro

Si su organización desea un enfoque que haga énfasis en los activos de información a partir del modelo Octave entonces debe ajustarse a los siguientes elementos.

Fase 1. Función de la dirección

- Desde la dirección de la organización se fijan los procedimientos para el análisis y valoración de los riesgos.

Fase 2. Caracterizar los activos

- Elaborar la caracterización de cada uno de los activos de la información.
- Determinar los recursos de información que tiene a su disposición la organización.

Fase 3. Determinar las amenazas a que se encuentra expuesta la plataforma

- Delimitar y establecer cuáles son las áreas del sistema susceptibles de ser atacadas por una amenaza.
- Establecer bajo qué condiciones se puede materializar una amenaza y qué tanto alcance puede tener.

Fase 4. Determinar los posibles riesgos y desplegar planes de mitigación

- Determinar a qué riesgos se encuentran expuestos los activos de información.
- Hacer una evaluación y análisis.
- Escoger e implementar enfoques y estrategias de mitigación del riesgo.

Por tratarse de un modelo que involucra muchos escenarios posibles, un elevado número de organizaciones aplican el modelo Octave para el análisis, evaluación y gestión de los riesgos informáticos. La imagen describe el proceso que desarrolla un modelo de análisis y gestión de riesgos basado en Octave.

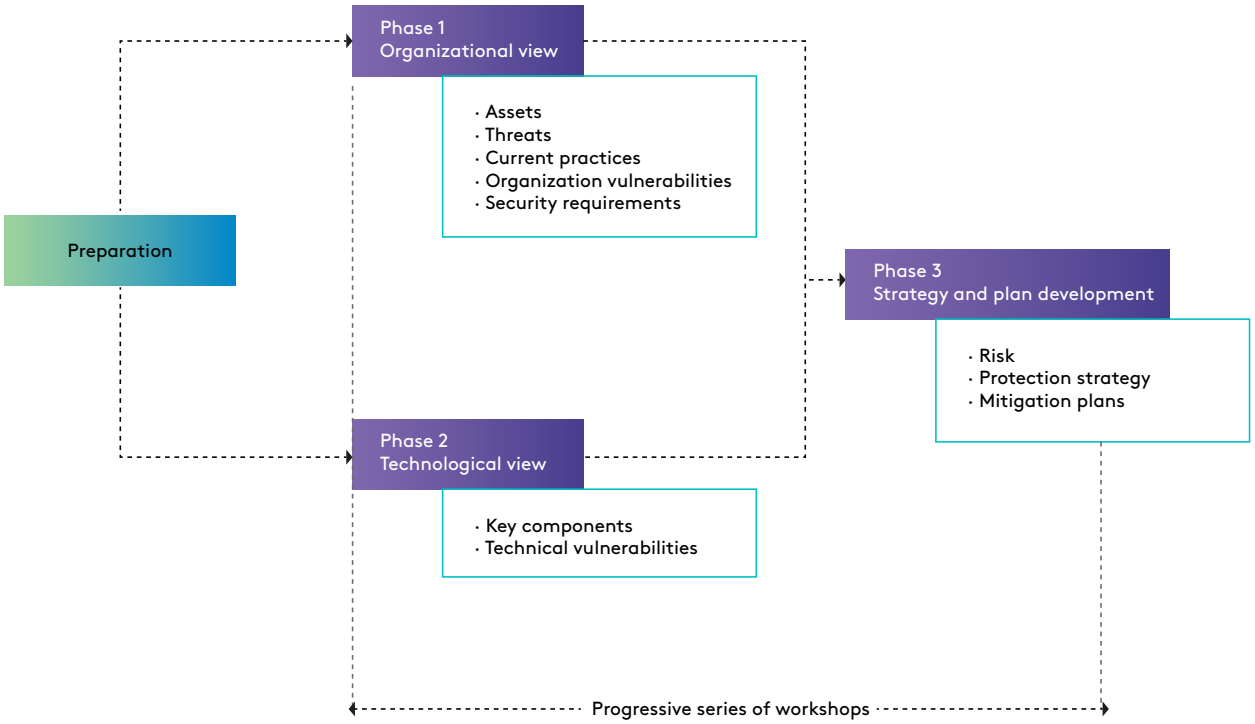


Figura 5. Modelo Octave
Fuente: Universidad de Carnegie Mellon (2007)

Algunos especialistas resaltan desventajas del modelo Octave porque consideran que requiere demasiados formatos o anexos.

Modelo Mehari

Mehari es un desarrollo del Club de la Seguridad de la Información Francés, este club es una organización de profesionales en seguridad de la información que trabajan de manera coordinada y mancomunada para intercambiar experiencias y desarrollar soluciones que brinden soporte y apoyo a las empresas para gestionar de forma adecuada sus plataformas de información a través de buenas prácticas y conocimientos técnicos avanzados.

En este orden de ideas (Clusif, 2010) define Mehari como un conjunto de instrumentos y procedimientos para una adecuada gestión de la seguridad de la información y los elementos relacionados con ella, a partir de un análisis de riesgos específico. En este sentido se puede considerar como un método para la evaluación y gestión del riesgo.

Se destacan de Mehari los siguientes elementos:

- Incluye un modelo de riesgos de orden cuantitativo y cualitativo.
- Examina la funcionalidad de las estrategias de seguridad que se encuentran en ejecución o las que están por implementarse.

- Incorpora extensiones para evaluar y simular los niveles de riesgo asociados a la incorporación de nuevos elementos al sistema.
- Incorpora bases de datos, conocimientos y manuales que describen los módulos de amenazas, riesgos y vulnerabilidades.
- Es desde el análisis que se hace para el presente curso el único modelo que busca estar alineado con las normas ISO 27001 y 27005.

Dentro de los objetivos para incorporar el método en una organización se destacan:

- Elaborar un diagnóstico preciso del estado de la seguridad en los sistemas de gestión de información al interior de la organización.
- Hacer un análisis en detalle de las afectaciones que una seguridad poco robusta pueda causar sobre los objetivos de la organización: "intereses implicados".
- Hacer un análisis preciso y evaluación de los riesgos asociados a un sistema de información.

Por las condiciones bajo las cuales se concibe el modelo y su énfasis en el análisis y evaluación del riesgo, su implementación está orientada casi que de forma exclusiva al SGSI así:

- Determinar y delimitar el contexto y alcance del SGSI.
- Establecer una clasificación de activos según su tipo y la categoría, principales o secundarios.
- Efectuar el análisis de los activos y sus respaldos, identificar en ellos las vulnerabilidades potenciales e inherentes a la naturaleza del activo.
- Determinar o estimar los daños que puede sufrir el activo si se materializa una amenaza. En este ítem estimar los posibles escenarios de riesgo para el activo.
- Hacer el análisis de todos los escenarios asociados a una posible amenaza que se materializa, contexto, actores, cómo se inicia, qué sucede mientras se desarrolla y las condiciones antes y después de su materialización.
- Descripción de los elementos de control y mitigación de los riesgos, qué procedimientos de seguridad se implementan y las ventajas que conllevan para la compañía.

Este modelo puede ser usado en cualquier tipo de organización independiente de su tamaño, naturaleza y ámbito de negocio. Sin embargo, algunos expertos señalan desventajas en su diseño como las que se mencionan más adelante:

- Se orienta a condiciones de la información como la confidencialidad, integridad y disponibilidad sin tener en cuenta condiciones como autenticación de usuarios o el "no repudio".
- Los controles no se incluyen como parte del análisis del riesgo y se incorporan en la gestión.
- El proceso de gestión se hace denso y complejo de manejar porque incluye controles e impacto.

Modelo Coras

Su nombre es el acrónimo de las palabras Construct a Platform for Risk Analysis of Security Critical System: construcción de una plataforma para el análisis de riesgos de sistemas de seguridad crítica. La primera versión de este modelo se publicó el año 2001 por una organización de investigación del Gobierno noruego financiada por la comunidad europea y organizaciones públicas y privadas. Este método se destaca porque incluye:

- Está compuesto por siete pasos.
- Incluye análisis de riesgos basado en modelos que se construyen bajo lenguaje UML.
- Un lenguaje de programación propio diseñado bajo UML.
- Soporta la elaboración de modelos gráficos bajo Microsoft Visio.
- Incluye biblioteca de casos de uso.
- Los casos se pueden guardar y reutilizar, además incorpora una biblioteca con casos de ejemplos disponibles para su uso.
- Incorpora formatos estandarizados de informes para hacer posible una comunicación fluida entre distintos actores del proceso.

En este sentido, apreciados estudiantes, existen múltiples metodologías que se han propuesto para el análisis y evaluación de los riesgos de la seguridad de la información, a continuación, se enuncian algunos métodos con su descripción y origen y será un compromiso de su parte profundizar en sus características.

Método Ebios

Este método se desarrolla y publica por el gobierno francés, incorpora un *software* para el apoyo del diseño e implementación del sistema. Su diseño se publica en 1995 por la Secretaría de Seguridad. Su nombre significa expresión de necesidades e identificación de objetivos de seguridad.

Modelo Nacional de Gestión del Riesgo de Seguridad Digital

En el año 2017 el Gobierno de Colombia diseña y expide un modelo de gestión de riesgos digitales orientado a todas las organizaciones del sector público y privado para que incorporen prácticas que tiendan al análisis, evaluación y mitigación de riesgos inherentes a la seguridad digital en Colombia. Este modelo se desarrolla a partir de los lineamientos emitidos por el Consejo Nacional para la Política Económica y Social, que en su documento Conpes 3854 de 2011, establece para el país una "política nacional de seguridad digital" que se orienta a fortalecer el crecimiento y desarrollo económico del país y en especial de la economía digital.

Lectura complementaria

Para finalizar realice la lectura complementaria:

Modelo Nacional de Gestión de Riesgos de Seguridad Digital

Ministerio de Tecnologías de la Información y Comunicaciones

De esta manera, apreciados estudiantes, concluimos el estudio de los modelos que nos ayudan al análisis, evaluación y gestión de los riesgos informáticos en cualquier escenario de nuestro entorno profesional o laboral.

A continuación, los invito a diseñar un modelo de acuerdo a las particularidades de algunos contextos específicos por medio de la actividad evaluativa: prueba objetiva individual.

Nos encontramos en el eje cuatro. ¡Hasta pronto!

BIBLIOGRAFÍA

Caralli, R., Stevens, J., Young, L., y Wilson, W. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Recuperado de https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

Fernández, M. (2003). Estudio de una estrategia para la implantación de los sistemas de gestión de la seguridad de la información. (Tesis doctoral). Universidad de Cádiz, España.

INCIBE. (2015). Gestión de riesgos. Una guía de aproximación para el empresario. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

ISO. (2013). ISO 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. Recuperado de https://www.iso.org/standard/54534.html

ISO. (2018). ISO 27005:2018. Information technology - Security techniques - Information security risk management. Recuperaado de https://www.iso.org/standard/75281.html

ISO. (2018). ISO 31000:2018. Risk management – Guidelines. Recuperado de https://www.iso.org/standard/65694.html

Ministerio de Hacienda y Administración Públicas. (2012). MAGERIT V3. Metodología de análisis y gestión de riesgos de los sistemas de información. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VVBx5WPsoco

Molina, M. (2000). *Seguridad de la información. Criptología*. Miami, EE. UU.: El Cid Editor.

Mogollón, A. (2008). Análisis comparativo: metodologías de análisis de riesgos. Recuperado de http://www.academia.edu/14195886/An%C3%A1lisis_Comparativo_Metodolog%C3%ADas_de_an%C3%A1lisis_de_Riesgos

NIST. (2012). Guide for conducting risk assessment. Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf