Indicadores para la evaluación y toma de decisiones sobre la gestión de riesgos en activos informáticos en la Universidad Nacional de Río Negro

Peña, Ricardo Luis; Lugani, Carlos Fabián

{rlpena; clugani} @unrn.edu.ar

Universidad Nacional de Río Negro, Sede Atlántica
Laboratorio de Informática Aplicada

Resumen. Luego de la aplicación del proceso de gestión de riesgos en los activos informáticos de la organización, resulta necesario determinar en qué medida el mismo fue efectivo y tomar decisiones en consecuencia. En este trabajo se describen los principales factores de decisión con respecto a la gestión de riesgos informáticos y, a partir de estos, se desarrollan diversos indicadores de desempeño. En consideración a estos últimos, se describe una metodología orientada a calcular el rendimiento del proceso de gestión de riesgos informáticos de forma cuantitativa y objetiva mediante la determinación de un índice que expresa el porcentaje de tal desempeño. Por último, se presenta el tablero de control destinado a visualizar los resultados obtenidos. De esta manera, se complementa el esquema de Gestión de Riesgos elaborado por Lugani y Peña (2018) en el trabajo Desarrollo de un esquema de Gestión de Riesgos Informáticos en la Universidad Nacional de Río Negro, y completado por los autores en Monitoreo de riesgos de activos de información en la Universidad Nacional de Río Negro.

Palabras clave: activos informáticos, indicadores de desempeño, toma de decisiones, Índice de Gestión de Riesgos, Puntuación Z, Proceso Analítico Jerárquico, tablero de control.

1 Introducción

El presente trabajo tiene por objetivo conceptualizar el uso de indicadores de desempeño como herramienta para evaluar la efectividad de la aplicación del esquema de gestión de riesgos informáticos de cuatro fases desarrollado para la Universidad Nacional de Río Negro. Asimismo, determinar el nivel de riesgo y respuesta a los mismos en que se encuentra actualmente la organización y brindar la información necesaria para la toma de decisiones. El auge y la constante sofisticación de los inci-

dentes informáticos actuales, y el consecuente aumento en la demanda de ciberseguridad, han llevado a organizaciones a aplicar metodologías que les permitan gestionar proactivamente los riesgos asociados a estas amenazas, a fin de reducir o mitigar tales eventualidades. La gestión de riesgos en activos informáticos es cíclica, y en consecuencia, mejora continuamente adaptándose a las necesidades cambiantes de seguridad de la información. Mediante el monitoreo y la evaluación del proceso implementado, es posible realizar un análisis del mismo y determinar su efectividad y el nivel de cumplimiento de los objetivos propuestos. Tal indagación debe brindar información clara, objetiva y determinante para la toma de decisiones en la organización. Estas características pueden satisfacerse mediante la elaboración y uso de indicadores. Los mismos permiten medir el desempeño de la gestión de riesgos y compararlo con los indicadores previamente definidos, así como también estos indicadores de riesgos constituyen luego indicadores clave de desempeño. Por lo tanto se tiene una visión más objetiva que justifica la decisión que se toma con respecto a la clasificación de los riesgos según su impacto y ocurrencia así como de los controles aplicados. Los indicadores retroalimentan al proceso con información relevante para el posterior análisis del esquema de gestión de riesgos. En virtud de lo señalado, este trabajo pretende trasladar, mediante indicadores de desempeño, los resultados de la aplicación de la gestión de riesgos a aquella información que el área ejecutiva de la organización considera necesaria para justificar la inversión en ciberseguridad y tomar decisiones en consecuencia.

1.1. Esquema de cuatro fases para la gestión de riesgos informáticos

Lugani y Peña (2018) han desarrollado un esquema para gestionar los riesgos en activos informáticos a través de cuatro fases:

1. Análisis de riesgos. La actividad comienza con un relevamiento de los activos informáticos y los riesgos asociados a estos, se calcula la criticidad de los mismos en función de su probabilidad de ocurrencia e impacto, y se evalúan las estrategias de respuesta.
2. Diseño del tratamiento de los riesgos. Una vez identificados los riesgos, es necesario definir medidas para reducirlos o mitigarlos, desarrollando los

controles de seguridad necesarios y planificando la respuesta a los eventos de seguridad.

3. Implementación del tratamiento de riesgos. El equipo responsable de la seguridad en la organización aplica las medidas definidas previamente.
4. Monitoreo y evaluación. La gestión de riesgos no concluye en la implementación, sino que continúa a través del seguimiento de los riesgos y los planes de respuesta implementados (PMO Informática, 2012). Por ello, es necesario registrar los resultados obtenidos durante y después de la actividad, a fin de verificar su efectividad.

La Figura 1.1 resume el esquema de cuatro fases y su relación, demostrando ser un proceso continuo.

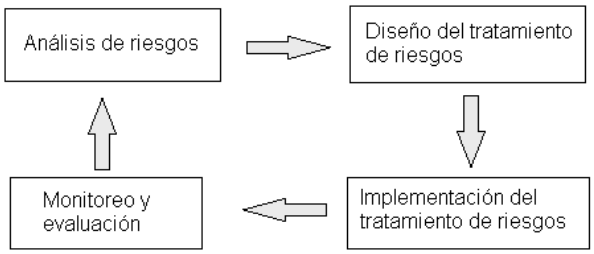

Figura 1.1. Esquema de cuatro fases para la gestión de riesgos informáticos.

2. Toma de decisiones y la gestión de riesgos informáticos

El correcto desempeño de una organización exige de la misma un proceso continuo de toma de decisiones importantes, que le permitan reducir posibles riesgos, dar solución a los problemas existentes y aprovechar las oportunidades de negocio que se presenten. Por consiguiente, este proceso requiere la capacidad de analizar, evaluar, reunir alternativas y considerar variables a fin de encontrar soluciones razonables (Villanueva Flores, 2015). Estas soluciones suelen orientarse a aumentar la eficiencia, es decir, alternativas que impliquen la máxima efectividad mediante la optimización de recursos (relación costo-beneficio). La toma de decisiones abarca las distintas áreas de la organización, e incluyen alternativas de estrategias y objetivos a largo plazo (estratégicas), los planes de acción para su cumplimiento (tácticas) y la eficiencia del proceso para implementar los mismos (operativas). Por lo anterior, es

fundamental que las decisiones estén respaldadas por información exacta, oportuna y confiable. Una fuente de información con tales características no sólo permite a la organización una mejor percepción de la situación actual, sino también la identificación de las alternativas que son viables y aquellas que no. En consecuencia, mediante decisiones acertadas, la organización no sólo genera un mejor posicionamiento en su ambiente de negocios sino también crea capacidades que les permitan orientarse a los cambios y adaptarse a ellos (Rodríguez Cruz, 2015). De esta manera, es importante destacar entonces que una buena toma de decisiones encuentra sustento en la información precisa y fiable.

En correspondencia con lo señalado anteriormente, la gestión de riesgos informáticos también requiere de variables que permitan a la organización evaluar la viabilidad del proceso y tomar decisiones en consecuencia. Estos factores abarcan los riesgos tratados, la efectividad de los controles aplicados, la ocurrencia de incidentes de seguridad y las potenciales pérdidas económicas. Para el esquema de gestión de riesgos de cuatro fases desarrollado por Lugani y Peña (2018), se definieron los siguientes factores de decisión:

- Cantidad de riesgos tratados e ignorados. Conocer cuántos riesgos fueron tratados constituye la base para analizar las demás variables, y permite conocer qué tan consolidado se encuentra el proceso actual para abordar los riesgos en la organización (cuántos riesgos es capaz de tratar dentro de los identificados). No obstante, es útil conocer además aquellos riesgos que fueron ignorados en el proceso. Estos suelen relacionarse con amenazas de menor criticidad, e identificarlos permite conocer el grado de tolerancia a los riesgos en la organización actualmente (cuántos es capaz de asumir).
- Controles aplicados efectivamente. Es preciso destacar que el desarrollo de controles de seguridad diferencia el diseño del mismo de su ejecución. Inicialmente, una medida de seguridad debe ser definida (puede distinguirse incluso esta fase como una etapa temprana), determinando qué medida realizar para responder al riesgo. A esta actividad le sucede el diseño del control, esto es, precisar las acciones y recursos concretos que inter-

vendrán para abordar el riesgo de acuerdo a lo definido. Asimismo, el diseño del control es diferente a la aplicación efectiva del mismo, esto es, el riesgo no se verá reducido hasta que se haya ejecutado (probado) el control. Ha de mencionarse que estas etapas deberían ser excluyentes entre sí: un control no puede ser (re)diseñado mientras se está ejecutando, puesto que se dificultaría determinar la efectividad del diseño anterior. Un control debería finalizar su ejecución a fin de evaluar su capacidad de respuesta y, en consecuencia, corroborar la precisión del diseño del control aplicado. Por lo anterior, conocer aquellos controles que fueron ejecutados y brindaron los resultados deseados sobre los riesgos permite a la organización determinar el grado de capacidad de las respuestas definidas.

- Controles no efectivos. De igual manera que con los controles efectivos, es necesario determinar aquellos que fueron ejecutados y cuyos resultados no fueron los esperados. Los mismos le permiten a la organización conocer el grado de ineficacia en el diseño de los controles, a fin de efectuar una revisión de los mismos.
- Riesgos residuales. La aplicación de los controles no siempre logra reducir o mitigar el riesgo, quedando un remanente de este, conocido como riesgo residual. Debido a que no es posible tener la completa certeza de que un evento de seguridad nunca sucederá, considérese inevitable la existencia de este tipo de riesgos. Por ello, la organización debe conocer los mismos a fin de mantener un equilibrio entre los recursos y mecanismos dedicados a minimizar los riesgos, y un nivel de confianza o tolerancia suficiente (Rodríguez, 2014). Este análisis determinará si aceptar el riesgo o invertir recursos en mejorar los controles existentes o incluso, añadir nuevas medidas de respuesta. Aquellos riesgos cuyos controles no han sido ejecutados no se han visto reducidos ni mitigados y, por consiguiente, deben considerarse en esta área de decisión.
- Eventos de seguridad ocurridos. Durante el proceso en el que se implementa la gestión de riesgos pueden suceder incidentes de seguridad relacionados con los activos informáticos. Analizar el origen de estas eventu-

alidades resulta útil para determinar su relación con riesgos no identificados, la aplicación de controles ineficaces, nuevos controles aún no definidos ni ejecutados, o riesgos residuales.

- Pérdida o potencial pérdida de dinero por la ocurrencia de eventos. Es necesario determinar el costo económico producido por la ocurrencia de un incidente de seguridad. Este costo depende de factores como el valor del activo, el tiempo de inactividad de este o del proceso de negocio, los recursos necesarios para la recuperación y la inversión en futuros controles con el fin de evitar la repetición de la eventualidad. Este costo resulta, lógicamente, en una pérdida (o potencial pérdida) de dinero para la organización.
- Dinero asegurado por la protección de activos. Así como la pérdida de dinero por la ocurrencia de eventos de seguridad, se debe calcular además la cantidad de dinero que se asegura con aquellos activos en riesgo que disponen de controles aplicados. Al comparar este valor con el costo originado por eventualidades, la organización podrá analizar la viabilidad económica de la gestión de riesgos.

La indagación de los factores de decisión mencionados conduce a determinar el nivel de riesgo actual en que se encuentra la organización y la capacidad de respuesta del esquema de gestión de riesgos. De igual manera que la matriz de probabilidad e impacto para la visualización de los riesgos y su criticidad, se desarrolló un tablero de control que permite graficar el desempeño del mencionado esquema.

3. Indicadores de desempeño para la gestión de riesgos informáticos

Como se mencionó anteriormente, una correcta toma de decisiones implica la disposición de información precisa y confiable, que es posible obtener mediante el desarrollo y uso de indicadores. Estos últimos son variables o datos que permiten medir de forma concreta el estado actual de un aspecto importante y determinar su evolución. Al brindar información cuantitativa, los indicadores también favorecen la comparación entre sí, lo que permite desarrollar y/o fundamentar criterios de forma

objetiva, que influyen en las decisiones a tomar. Un tipo de indicador ampliamente utilizado es aquel que mide el desempeño, conocido como Indicador Clave de Desempeño (KPI), que permite conocer el resultado de un proceso en función de cumplimiento de objetivos, recursos utilizados y errores cometidos. La consecución de los indicadores de desempeño en actividades que agregan valor al negocio puede generar una fuerte influencia en el desarrollo de la organización, revelando además aquellos puntos a mejorar, necesarios en cada proceso (Ortega, 2018).

A fin de evaluar el rendimiento del esquema de gestión de riesgos en 4 fases definido por Lugani y Peña (2018), se desarrollaron dos clases de indicadores, de acuerdo al público al que van dirigidos:

- De gestión. Tienen la finalidad de evaluar el desempeño global del esquema definido, aplicado en la organización. Están orientados al área ejecutiva o de gestión, y se sustentan en los factores de decisión mencionados anteriormente. Por ello, analizan la efectividad del esquema en términos de cumplimiento de objetivos, nivel de fallos y optimización de recursos.
- De sistemas. Su objetivo es evaluar el rendimiento de los activos en términos específicos de los mismos. El área de Sistemas debe acceder a información característica de los activos que estos utilizan, de forma tal que puedan medir el desempeño de los mismos en relación a su funcionamiento, costo, nivel de servicio y satisfacción del usuario. A su vez, los indicadores de sistemas constituyen una base para el área de gestión, puesto que es su valor el que determina la efectividad (o no) de los controles aplicados a los activos. Estos indicadores permiten ser utilizados para ser analizados y comparados con KPI pasados, sirviendo los primeros a su vez al relevamiento inicial del esquema de 4 fases. Estos indicadores fueron relevados con el responsable de Redes e Infraestructura de la Universidad Nacional de Río Negro.

En virtud de lo señalado, los indicadores de gestión permiten determinar el nivel de riesgo actual en la organización y por ende el porcentaje de efectividad del esquema de 4 fases. No obstante, se requieren los indicadores de sistemas para evaluar si los controles aplicados fueron o no efectivos, proporcionando un respaldo del área informática en la toma de decisiones. Las tablas 3.1 y 3.2 detallan los indicadores de

gestión y sistemas desarrollados respectivamente; no se descarta la aparición de nuevos indicadores o supresión de algunos de los mencionados en el presente artículo a medida que este esquema se desarrolle en el tiempo.

Indicador	Fórmula	Categoría
Porcentaje de riesgos abordados	Nº de riesgos con controles asociados / total riesgos	Reducción del riesgo
Porcentaje de riesgos ignorados	(1 - porcentaje de riesgos abordados)*100	Reducción del riesgo
Porcentaje de efectividad de controles	Nº de controles ejecutados satisfactoriamente / total controles ejecutados	Reducción del riesgo
Porcentaje de controles no efectivos	100 - porcentaje de efectividad de controles	Reducción del riesgo
Porcentaje de controles aplicados	Controles ejecutados / total de controles definidos	Reducción del riesgo
Porcentaje de controles no aplicados	100 - porcentaje de controles aplicados	Reducción del riesgo
Porcentaje de riesgos críticos	Nº de riesgos críticos / total de riesgos	Identificación del riesgo
Nº de riesgos residuales	Nº de riesgos con criticidad >0 + riesgos no tratados	Identificación del riesgo
Nº de eventos de seguridad concretados	-	Respuesta a incidentes
Porcentaje de previsibilidad de eventos	Nº de eventos ocurridos registrados como potencial riesgo / total de eventos ocurridos	Respuesta a incidentes
Dinero potencialmente perdido por ocurrencia de eventos de seguridad	Valor monetario de riesgos relacionados con eventos ocurridos + costo de eventos ocurridos sin riesgo registrado	Factor financiero
Dinero potencialmente ahorrado (dinero que se ahorraría con todos los riesgos controlados)	Valor total de activos en riesgo / valuación total de activos	Factor financiero

Tabla 3.1. Indicadores de desempeño de la gestión de riesgos.

Indicador	Fórmula
Cantidad de ancho de banda consumido	-
Puertos abiertos	-

Origen de conexiones (conexiones de salida)	-
Nº de conexiones en horarios no habituales	-
Existencia de Acuerdos de Nivel de Servicio (SLA)	-
Tiempo de actividad o disponibilidad	-
Cantidad de aplicaciones sin actualizar a la última versión	-
Cantidad de interrupciones del servicio	-
Cantidad de accesos incorrectos	-
Numero de nuevas entradas en la lista de intrusos en HIDS[1] y/o NIDS[2]	-

Tabla 3.2. Indicadores de rendimiento de activos informáticos.

3.1. Cálculo del nivel de riesgo informático

Mediante estos indicadores se llega a un único valor determinante que se focaliza en forma objetiva en el rendimiento del proceso de gestión de riesgos aplicado en la organización. Para ello, se utilizó como base el denominado Índice de Gestión de Riesgos de Desastres desarrollado por Carreño, Cardona, Marulanda y Barbat (2006). El IGR fue elaborado con el fin de evaluar el desempeño de la gestión de riesgos de desastres en el ámbito de políticas públicas de los países latinoamericanos. No obstante, resulta útil para aplicar a los riesgos informáticos, puesto que se vale de indicadores y factores de decisión similares a los explicados en este artículo.

Con base en Carreño et al. (2006), el IGR para activos informáticos es calculado como el promedio de cuatro subíndices o indicadores compuestos:

- Identificación del riesgo. Indica la percepción colectiva del riesgo, a partir del relevamiento y evaluación de los activos informáticos y los riesgos a los que estos están expuestos. A su vez, los riesgos identificados (y su criticidad inherente) deben ser dimensionados y representados a fin de reconocerlos.
- Reducción del riesgo. Corresponde a la definición y aplicación de los controles de seguridad con el objeto de reducir los riesgos identificados y su potencial impacto.
- Recuperación de incidentes. Involucra las acciones realizadas posteriormente a la ocurrencia de eventos de seguridad, con el fin de revelar el nivel de preparación de la organización frente a dichos eventos.

[1] HIDS Host-Based Intrusion Detection System o Sistema de Detección de Intrusos en Host
[2] NIDS Network Intrusion Detection System o Sistema de Detección de Intrusos en Red

- Factor financiero. Indica el efecto del proceso de gestión de riesgos en términos económicos, permitiendo saber las potenciales pérdidas por la ocurrencia de eventos de seguridad, así como también el potencial ahorro de dinero por la reducción de los riesgos identificados.

Para el cálculo del IGR informático se utilizaron los indicadores de gestión desarrollados anteriormente, categorizados dentro de los subíndices mencionados, tal como se muestra en la Tabla 3.1. Esta división en áreas específicas facilita la comprensión del rendimiento del proceso implementado, y permite además analizar en qué factor/es la organización debería invertir en mayor y menor medida.

En primer lugar, es necesario normalizar los indicadores de acuerdo a alguna escala común de valores para poder establecer criterios de comparación entre los mismos. La escala utilizada para el IGR informático se compone de valores del 1 al 5, que evalúan el desempeño del indicador desde bajo a óptimo respectivamente. La Tabla 3.3 presenta la escala la mencionada escala de desempeño.

Nivel de desempeño	Puntaje asociado
Bajo	1
Incipiente	2
Apreciable	3
Notable	4
Óptimo	5

Tabla 3.3. Escala de desempeño de indicadores.

Luego se aplica la normalización en los indicadores utilizando el método de Puntaje Z o Z-Score, que permite determinar la distancia de cada valor con respecto a la media. El proceso comprendido en este método es el siguiente:

1. A partir de los valores de desempeño asignados a los indicadores, se calcula la media y la desviación estándar de la distribución normal.
2. Cada valor de desempeño es restado a la media obtenida en el primer paso.
3. Cada resultado del paso anterior es dividido por la desviación estándar, obteniendo en cada caso un valor de z. El conjunto de valores de z obtenidos corresponde a los indicadores normalizados, utilizados para calcular el rendimiento de cada subíndice.

Además de la calificación mencionada y su correspondiente normalización, es necesario establecer pesos o prioridades relativas entre los indicadores de cada subíndice, lo que permite determinar aquellos de mayor importancia dentro de la toma de decisiones en cada factor. De esta manera, es posible analizar cuál fue el desempeño de los principales indicadores, es decir, de aquellos con mayor peso. Realizar el cálculo de tales prioridades requiere de un análisis de variables múltiples, a fin de determinar la relevancia de cada indicador en relación a cada criterio especificado. Para el IGR informático, se consideraron tres criterios o variables de análisis:

a. Relevancia. Qué tan relevante para la toma de decisiones es la información del indicador.
b. Trazabilidad. Cuán fácil es rastrear la información presentada por el indicador.
c. Especificidad. Qué tan específica es la información proporcionada por el indicador.

Los mismos son utilizados para determinar los pesos en cada subíndice. Para ello, se resolvió utilizar el método de Proceso Analítico Jerárquico o AHP, que consiste en seleccionar alternativas a un problema u objetivo en función de criterios definidos en forma jerárquica. Para este método es fundamental que los criterios sean bien definidos, relevantes y mutuamente excluyentes (Yepes Piqueras, 2018). El objetivo es la raíz de la jerarquía, sus nodos hijos representan los criterios o variables definidas, y los nodos inferiores las alternativas (indicadores). La Figura 3.1 presenta la jerarquía para el análisis de los indicadores del subíndice Identificación de Riesgos. Cabe mencionar que tanto el objetivo como los criterios deben tener asignado un determinado puntaje, y que la suma de los puntajes de los criterios de un mismo nivel debe ser igual al puntaje del nodo superior

Para las jerarquías de los subíndices del IGR informático se estableció el puntaje del objetivo igual a 1.

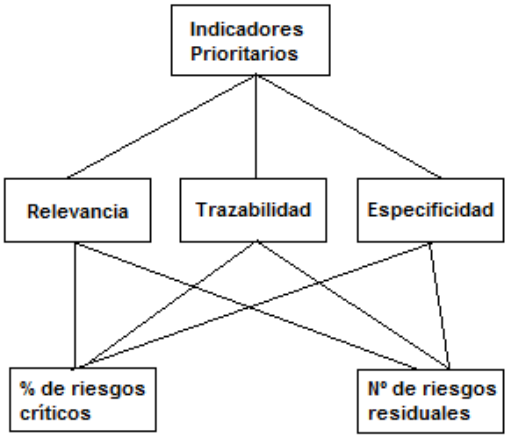

Figura 3.1. Jerarquía para el análisis multicriterio de indicadores de Identificación de Riesgos

Haciendo uso de la jerarquía definida, se procede a comparar los criterios entre sí, y luego los indicadores de a pares utilizando matrices de comparación, para cada criterio definido. Para esta tarea se requiere una escala de importancia, del 1 al 9, donde 1 señala igual importancia entre ambos elementos (indicadores), mientras que 9 indica que el elemento *a* es 9 veces superior al elemento *b*. La escala se completa con los valores 1, 3, 5, 7 y 9, mientras que los números pares son requeridos sólo en situaciones intermedias. Mediante la técnica de vectores propios, se calculan los pesos relativos de los indicadores, donde una de sus ventajas es que verifica la consistencia de la matriz de comparación utilizando valores propios (Carreño et al., 2006).

Una vez calculados los pesos relativos de los indicadores, es posible determinar el desempeño de cada subíndice mediante la siguiente ecuación propuesta por los autores citados:

$$IGR_{(1,2,3,4)} = \frac{\sum_{i=1}^{n} (w_i I_i)}{\sum_{i=1}^{n} w_i} \times 100 \quad (1)$$

Donde w_i es el peso relativo de cada indicador, mientras que I_i corresponde a su valor normalizado. Por último, es IGR informático es calculado como el promedio de los subíndices desarrollados anteriormente, es decir:

$$IGR = \frac{IGR_1 + IGR_2 + IGR_3 + IGR_4}{4} \quad (2)$$

Finalmente, este último valor es utilizado por la organización como el porcentaje de efectividad del esquema de gestión de riesgos y, en consecuencia, resulta indispensable para la toma de decisiones. El empleo de la normalización estadística y la determinación de pesos relativos mediante el análisis AHP brindan una mayor consistencia al IGR puesto que los indicadores no sólo son relacionados en una escala común, sino también priorizados mediante criterios de evaluación bien definidos. Esta consistencia contrarresta la rigurosidad de la metodología, y la información es más exacta que la obtenida por métodos más simples, como por ejemplo promediar los valores de desempeño de los indicadores.

3.2. Representación en el tablero de control

La comprensión del desempeño de la gestión de riesgos a partir de los indicadores evaluados es mayor si tal información es visualizada mediante un tablero de control. Este último consiste en representaciones gráficas del estado de indicadores en relación al cumplimiento de los objetivos propuestos en un área determinada, lo que permite a la mesa ejecutiva diagnosticar el rendimiento actual de la organización y adoptar estrategias y decisiones en consecuencia. De esta manera, la información puede ser agrupada de acuerdo a ciertos objetivos, facilitando la comparación de los indicadores relacionados a una meta determinada y tomar decisiones en función de la misma. Por ello, la organización debería adoptar un enfoque agrupado que permita un consenso en todos los aspectos, aumentando la probabilidad de lograr un progreso significativo (Subramanian, 2015). En virtud de lo señalado, considérese de utilidad disponer de un tablero de control en el que el área ejecutiva o de gestión pueda diagnosticar dinámicamente el desempeño organizacional y tomar decisiones.

Se desarrollaron herramientas de visualización del desempeño de la gestión de riesgos informáticos que, en su conjunto, conforman un tablero de control. Considerando una estructura jerárquica de acuerdo al nivel de abstracción de la informa-

ción presentada, en primer lugar se representa el IGR informático, utilizando un gráfico de "termostato". En el mismo, se utilizan los colores de semáforo de acuerdo al valor del índice y mediante la escala presentada en la Tabla 3.4. Este estilo visual permite identificar rápidamente el valor del índice de desempeño actual, a la vez de verificar si el mismo es satisfactorio o no.

Nivel	Valor	Color asociado
Bajo	<=30%	
Medio	>30% y <=70%	
Alto	>70%	

Tabla 3.4. Escala de valores para el IGR informático.

La Figura 3.2 muestra la estructura del gráfico mencionado. En el segundo nivel del tablero, se presentan los cuatro subíndices del IGR, y son visualizados utilizando la misma estructura, es decir, la del termostato.

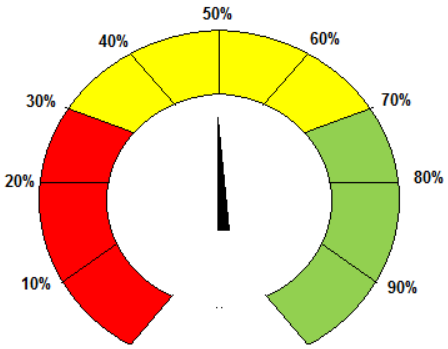

Figura 3.2. Gráfico de termostato para evaluar el IGR informático.

En el tercer nivel de la jerarquía se presentan los indicadores de gestión para cada subíndice mediante el uso de una tabla, con los siguientes valores:

- Nombre del indicador.
- Valor del indicador.
- Peso del indicador. La prioridad del indicador dentro del subíndice.
- Objetivo. La meta propuesta para el indicador correspondiente. Este también puede ser un objetivo conjunto, es decir, que involucre más de un indicador.
- Valor de desempeño. El rendimiento del indicador en función a la escala presentada en la Tabla 3.3.

- Color de desempeño. Presenta el color de semáforo correspondiente al valor de desempeño del indicador, siendo los puntajes 1 y 2 de color rojo, 3 amarillo, y 4 y5 de color verde.
- Responsable. El individuo o área que debe brindar respuestas en relación al indicador.

Haciendo uso de estas representaciones de la información, se elaboró finalmente el tablero de control de gestión de riesgos informáticos, tal como se muestra en la Figura 3.4. En el mismo se define un cuadrante por cada subíndice, con su valor de rendimiento actual y la tabla de indicadores correspondientes a esa categoría, mientras que en el centro del tablero se dispone el termostato con la información relacionada con el índice de desempeño general de la gestión de riesgos. Adicionalmente, en este último apartado, se incluye la evolución histórica del desempeño y el nivel de riesgo actual de la organización representado por un semáforo que enciende la luz correspondiente a este nivel (rojo=alto, amarillo=medio y verde=bajo). Esta información le permite a la organización saber en qué situación de riesgo está y qué tan preparada se encuentra para afrontarlo, así como también diagnosticar la evolución del proceso.

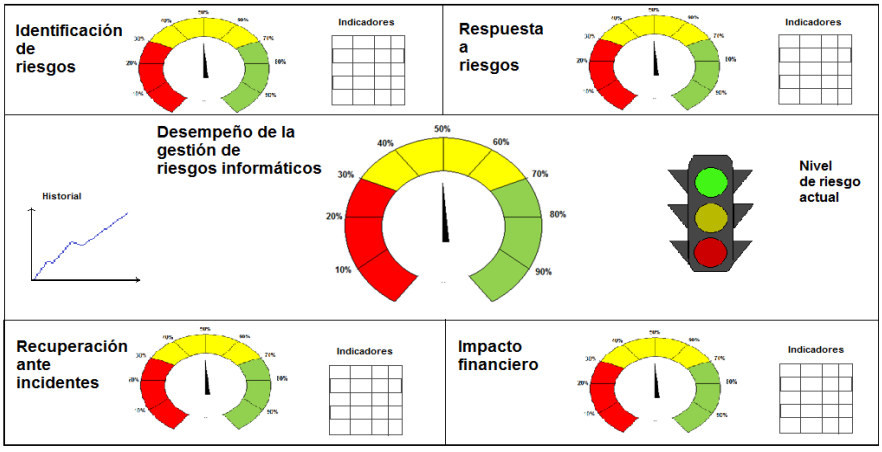

Figura 3.3. Boceto de tablero de control de gestión de riesgos informáticos.

Con la herramienta propuesta, el área ejecutiva de la organización podrá analizar rápida y dinámicamente el estado actual de la gestión de riesgos en sus activos infor-

máticos e incluso indagar con mayor detalle según descienda en la jerarquía de visualización del tablero. De esta manera, se podrá conocer aquellos indicadores cuyo desempeño cumplió con los objetivos definidos y aquellos que no lo hicieron, diagnosticando su influencia en el rendimiento general del proceso de gestión de riesgos. Por ello, se tomarán decisiones más orientadas e involucrarán a los distintos miembros responsables de los indicadores, mejorando a su vez la gobernanza organizacional.

4. Conclusiones

La evaluación del proceso de gestión de riesgos requiere de información objetiva, fiable y oportuna que facilite la toma de decisiones en la organización, además de ser determinantes para la misma. Estas características aplican a los indicadores de desempeño, que analizan el rendimiento en términos de objetivos cumplidos, uso eficiente de recursos y fallos cometidos. Para el proceso de gestión de riesgos en 4 fases, se determinaron en primer lugar aquellos factores importantes para la toma de decisiones, a fin de esclarecer las áreas de análisis de mayor relevancia. A partir de estos factores, se elaboraron indicadores de gestión y de activos, orientados de acuerdo al destinatario objetivo, que incluye al área ejecutiva de la organización y los responsables de Sistemas. Con base al Índice de Gestión de Riesgos de Desastres o IGR, se desarrolló una metodología de cálculo del desempeño total del proceso de 4 fases. La misma se sustenta en medidas estadísticas como la normalización mediante el puntaje z, así como de técnicas de análisis multicriterio como el Proceso Analítico Jerárquico o AHP para evaluar las alternativas existentes para cada variable definida. A pesar de su complejidad, esta metodología logra una mayor aproximación al desempeño real de la gestión de riesgos informáticos en la organización, y con ello la base sobre la cual tomar decisiones será más sólida y las decisiones más acertadas. Mediante el uso del tablero de control, la organización tendrá un balance continuo del proceso de gestión de riesgos, lo que le permitirá diagnosticar su estado y tomar decisiones bien enfocadas involucrando a aquellos miembros responsables del proceso.

5. Referencias

1. Carreño, M.L., Cardona, O.D., Marulanda, M.C. y Barbat, A.H. (2006). Índice para medir el desempeño de la gestión de riesgos. *Revista Internacional de Ingeniería de Estructuras, 11*(1),

25-44. Recuperado de http://idea.bid.manizales.unal.edu.co/documentos/13CarrenoIGR.pdf [Consultado 08 Dic., 2019]

2. Lugani, C.F. y Peña, R.L. (2018). Desarrollo de un esquema de Gestión de Riesgos para la Universidad Nacional de Río Negro. *Anales de SIE 2018, Simposio de Informática en el Estado, 47º Jornadas Argentinas de Informática e Investigación Operativa (JAIIO)*, 170-182. ISSN: 2451-7534. Recuperado de http://47jaiio.sadio.org.ar/sites/default/files/SIE-14.PDF [Consultado 08 Dic., 2019]

3. Ortega, O. (12 de Octubre de 2018). Indicadores de desempeño. Recuperado de https://trabajoypersonal.com/indicadores-de-desempeno/ [Consultado 04 Feb., 2020]

4. Peña, R.L. y Lugani, C.F. (2019). Monitoreo de riesgos de activos de información en la Universidad Nacional de Río Negro. *Anales de SIE 2019, Simposio de Informática en el Estado, 48º Jornadas Argentinas de Informática e Investigación Operativa (JAIIO)*, 1-11. ISSN: 2541-7534. Recuperado de http://170.210.201.137/pdfs/sie/SIE-01.pdf [Consultado 08 Dic., 2019]

5. PMO Informática. (15 de Octubre de 2012). *Cómo hacer el seguimiento de los riesgos en proyectos*. PMO Informática. Recuperado de http://www.pmoinformatica.com/2012/10/pasos-seguimiento-riesgos-proyecto.html [Consultado 10 Dic., 2019]

6. Rodríguez, I. (18 de Noviembre de 2014). ¿Qué es el riesgo, riesgo inherente y riesgo residual?. Recuperado de https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual [Consultado 13 de Dic., 2019]

7. Rodríguez Cruz, Y. (2015). Gestión de información y del conocimiento para la toma de decisiones organizacionales. Bibliotecas *Anales de investigación, 11*(1), 150-163. Recuperado de http://www.anales.bnjm.cu/index.php/anales/article/view/4386 [Consultado 10 Dic., 2019]

8. Subramanian, G. (2015). Corporate Governance 2.0. Harvard Business Review. Recuperado de https://hbr.org/2015/03/corporate-governance-2-0?language=es [Consultado 10 Mar., 2020]

9. Villanueva Flores, L. (4 de Marzo de 2015). La toma de decisiones en la organización y el gran valor del profesional de la información en su desarrollo. Recuperado de https://www.infotecarios.com/la-toma-de-decisiones-en-la-organizacion-y-el-gran-valor-del-profesional-de-la-informacion-en-su-desarrollo/#.Xe-8lMHPzIU [Consultado 10 Dic., 2019]

10. Yepes Piqueras, V. (27 de Noviembre de 2018). Proceso Analítico Jerárquico (Analytic Hierarchy Process, AHP). Recuperado de https://victoryepes.blogs.upv.es/2018/11/27/proceso-analitico-jerarquico-ahp/ [Consultado 19 Feb., 2020]