GESTIÓN Y ADMINISTRACIÓN DEL RIESGO EN LA ORGANIZACIÓN

Jiménez Higuera, Oscar Fernando.
Okim13@gmail.com
Universidad Piloto de Colombia

Resumen— Mediante el presente artículo se realiza un análisis sobre la *Gestión del Riesgo*, mediante el cual se establece una serie de procedimientos y actividades para determinar a través del análisis, identificación, evaluación del riesgo y la forma en que interactúan las personas frente al proceso de gestión y administración del mismo.

Abstract— Through this article it will make an analysis about the *Risk Management*, which process includes a series of process and activities in to determine through analysis, identification, risk evaluation and how people interact in the process of management and risk administration.

Índice de términos— Riesgo, causas, proceso, evento, consecuencia, probabilidad eficacia, análisis, amenaza.

I. INTRODUCCIÓN

Las organizaciones siempre se enfrentan a factores e influencias externas e internas por los constantes cambios de un mundo globalizado, el efecto de esta incertidumbre es el riesgo. Las organizaciones tienden a realizar su administración del riesgo a través de métodos como la identificación, análisis y evaluación del riesgo, con el fin de evitar la explotación de vulnerabilidades y garantizar que no se requiere tratamiento adicional del riesgo. Día a día la organización se enfrenta a constantes riesgos que pueden afectar su imagen comercial, afectando el contexto de la organización en la toma de decisiones por parte de las altas directivas.

Se entiende por riesgo la posibilidad de que suceda algo que afecte los objetivos de la organización o la probabilidad de materialización de una amenaza. Los riegos están en todos los procesos de la organización, los cuales pueden ser administrados con el objetivo de evitar, reducir, minimizar y ser transferidos. La administración y gestión del riesgo puede aplicar diversos métodos para identificar, analizar, evaluar y tratar los riegos. Durante el levantamiento de información es preciso conocer el comportamiento de la organización frente a cada uno de sus procesos con el fin de identificar amenazas que puedan afectar el correcto funcionamiento de la organización.

II. GESTIÓN Y ADMINISTRACIÓN DEL RIESGO

La gestión del riesgo es aplicable para toda la organización a través de procesos efectuados por la alta dirección y por todo el personal para proporcionar un aseguramiento al logro de sus objetivos propuestos.

Los riesgos se encuentran presentes en todos los procesos de la organización, sin embargo, pueden ser administrados por medio de proyectos y actividades que ayudan a garantizar que el riesgo se gestione eficaz, eficiente y coherentemente.

El enfoque de riesgos no se determina solamente con el uso de una metodología en particular, sino que también existen diferentes métodos para identificar, analizar, evaluar y tratar los riegos. Una característica clave es el establecimiento del contexto como una actividad que permite evaluar la naturaleza y la complejidad de sus riegos. Cuando se implanta la gestión del riesgo se permite a la organización efectuar las siguientes actividades:

- Aumentar la probabilidad de alcanzar los objetivos.
- Mejorar la presentación de informes.
- Asignar y usar eficazmente los recursos para el tratamiento del riego.
- Cumplir con requisitos legales y reglamentarios.
- Minimizar pérdidas.

Durante el proceso de evaluación del riesgo es necesario e importante cuantificar y priorizar los riegos frente a los criterios de aceptación y objetivos previamente definidos dentro de la organización. Cada uno de los resultados obtenidos determina la valorización del riesgo y las acciones a seguir.

Es pertinente realizar constantemente la evaluación del riesgo con el fin de identificar cambios en los requisitos de seguridad y en situaciones de riesgos como por ejemplo en activos, amenazas y vulnerabilidades para determinar cuándo se producen cambios significativos.

Antes de realizar el proceso de gestión del riesgo se debe definir un alcance claro y eficaz frente a las evaluaciones según sea lo apropiado. También es importante definir las necesidades de cada una de las partes participantes y establecer responsables del desarrollo de la política de gestión del riesgo.

Cada una de las actividades va relacionada al cumplimiento de los objetivos y metas de la organización en donde se busca crear y proteger el valor de esta.

De acuerdo con lo anterior, para realizar la actividad de análisis y administración de riesgos, utilizaremos el esquema en el proceso de administración del riesgo que se encuentra

basado en ISO31000:2009 como un modelo fuerte ante las actividades de identificación, análisis, evaluación y tratamiento del riesgo.

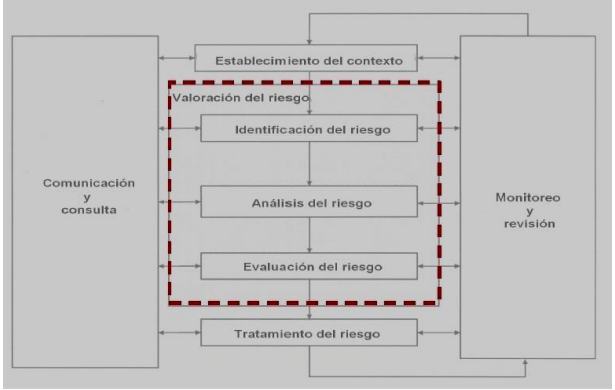


Figura 1. Establecimiento del contexto.
Fuente: ICONTEC, Instituto Colombiano de Normas Técnicas y Certificación. Norma Técnica colombiana NTC 5254, Primera edición de actualización. Proceso de Gestión de Riesgo ISO31000:2009.

A. Definición de clases de riesgos

Las organizaciones dentro de su proceso de identificación del riego realizan una clasificación que permite formular políticas que servirán como base para darles un tratamiento sobre el impacto o consecuencias que pueden ocurrir dentro de esta.

Debemos tener en cuenta que los riesgos no son sólo económicos y no sólo están relacionados con la tecnología, estos hacen parte del proceso de gestión del riesgo que se realice, por lo anterior podemos encontrar los siguientes tipos de riegos:

1) ***Riesgos estratégicos****:* Encaminados a la forma en que se administra la organización, enfocando sus riegos en asuntos de misión y cumplimiento de objetivos estratégicos y definición de políticas por parte de la alta gerencia.

2) ***Riesgos operativos:*** Están relacionados con el funcionamiento y la operación de los sistemas de información, procesos y funcionamiento entre dependencias.

3) ***Riesgos financieros:*** Relacionados con los recursos de la organización.

4) ***Riesgos de imagen:*** Tienen relación con la percepción y confianza de los clientes hacia la organización.

5) ***Riesgos tecnológicos:*** Asociados con la capacidad tecnológica de la organización.

B. Establecimiento del contexto

Las organizaciones se enfrentan constantemente a procesos de crecimiento tecnológico gracias a las necesidades requeridas por sus clientes; las inversiones que deben realizar en tecnología y analistas que prestan el servicio profesional son significativas, por lo que nace la necesidad de brindar mayor seguridad y administrar los riesgos en la organización. Por esto mismo, es importante definir cuáles son los procesos más críticos de la organización y asegurar una debida gestión y administración del riesgo.

C. Responsabilidades de la organización

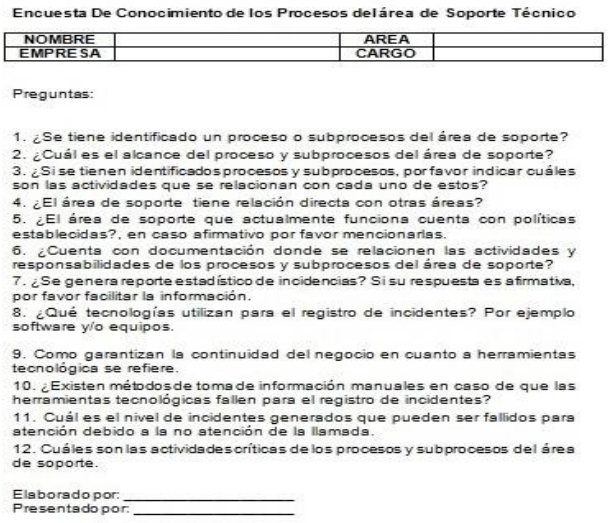
Es de vital importancia que la organización se responsabilice y apruebe los siguientes puntos para llevar a cabo la actividad de gestión del riesgo:

- Acceso a las instalaciones.
- Facilitar información requerida para realizar el análisis de riegos.
- Accesos lógicos al sistema de información.
- Accesos lógicos a las bases de datos de la organización.

D. Descripción del proceso

En la organización se establecen áreas que son el eje principal de la operación, estas se encargan de prestar los servicios de apoyo a otros procesos que pueden llegar a tener un impacto alto al quedar fuera de producción durante el ciclo diario de operaciones de la organización. Dentro de cada una de las áreas se identifican subprocesos que son de vital importancia y deben ser controlados con una debida gestión del riesgo.

Para realizar el levantamiento de información en cada uno de los procesos es necesario utilizar herramientas que ayudan en la recolección de datos, como por ejemplo el uso de encuestas, donde la información recolectada es producto del conocimiento de cada uno de los involucrados en el proceso.



Encuesta De Conocimiento de los Procesos del área de Soporte Técnico

NOMBRE		AREA	
EMPRESA		CARGO	

Preguntas:

1. ¿Se tiene identificado un proceso o subprocesos del área de soporte?
2. ¿Cuál es el alcance del proceso y subprocesos del área de soporte?
3. ¿Si se tienen identificados procesos y subprocesos, por favor indicar cuáles son las actividades que se relacionan con cada uno de estos?
4. ¿El área de soporte tiene relación directa con otras áreas?
5. ¿El área de soporte que actualmente funciona cuenta con políticas establecidas?, en caso afirmativo por favor mencionarlas.
6. ¿Cuenta con documentación donde se relacionen las actividades y responsabilidades de los procesos y subprocesos del área de soporte?
7. ¿Se genera reporte estadístico de incidencias? Si su respuesta es afirmativa, por favor facilitar la información.
8. ¿Qué tecnologías utilizan para el registro de incidentes? Por ejemplo software y/o equipos.
9. Como garantizan la continuidad del negocio en cuanto a herramientas tecnológica se refiere.
10. ¿Existen métodos de toma de información manuales en caso de que las herramientas tecnológicas fallen para el registro de incidentes?
11. Cuál es el nivel de incidentes generados que pueden ser fallidos para atención debido a la no atención de la llamada.
12. Cuáles son las actividades críticas de los procesos y subprocesos del área de soporte.

Elaborado por: _____
Presentado por: _____

Figura 2. Formato de encuestas para el levantamiento de Información dentro de la organización.
Fuente: autor.

Para algunas áreas de la organización también es de vital importancia los sistemas de almacenamiento en donde se resguarda la información de sus clientes y/o procedimientos de la organización. Por esto es menester la seguridad de la información en los almacenamientos de bases de datos.

Dentro de la organización es importante generar procesos de soporte, gestión y registro de incidentes, estas actividades son realizadas por las personas de las áreas de apoyo que a través de herramientas de gestión permiten el registro de actividades y solicitudes a cada una de las áreas de la organización. Esto hace posible registrar y documentar cada uno de los acontecimientos e incidentes generados dentro de la organización, los cuales son controlados a través de tickets de servicio que a su vez son utilizados para medir la efectividad de los servicios de apoyo.

A continuación se describen detalladamente las actividades relacionadas en los procesos de gestión de incidentes y soporte dentro de la organización:

TABLA I
PROCEDIMIENTO DE SOPORTE

Procedimiento	Descripción
Detección	Identificación de incidente
Registro	Recopilación de información y clasificación.
Diagnóstico	Análisis del incidente y programación de actividades para proveer solución.
Solución	Ejecución de actividades y atención al requerimiento, registro de actividades ejecutadas.
Finalización y cierre	Registro de actividades y confirmación de usuarios satisfechos.

Fuente: autor.

Dentro del proceso de prestación de servicios de apoyo se identifican los dos siguientes subprocesos.

El subproceso número uno se presenta al realizar el reporte generado en la herramienta de gestión de incidentes para atención del soporte de forma presencial frente al usuario final, durante la ejecución de este subproceso se realizan las siguientes actividades:

- Escalamiento del ticket al analista de help desk.
- Desplazamiento a las instalaciones del cliente para realizar soporte de primer nivel.
- Realizar validación y revisión del incidente presentado.
- Documentar las actividades realizadas durante el servicio.
- Realizar escalamiento a otras líneas de servicio cuando no es posible entregar solución a los incidentes.
- Seguimiento, control y cierre al servicio.
- Documentación y cierre del servicio.

El subproceso número dos se presenta cuando se comunican vía telefónica al área de soporte, en este caso es necesario gestionar información básica del usuario que realiza la solicitud, luego se procede a realizar el registro en la herramienta de gestión. En este subproceso se realizan las siguientes actividades:

- Solicitud del servicio vía telefónica.
- Validación de datos del usuario final.
- Identificación del tipo de requerimiento.
- Registro del servicio en la herramienta de gestión.
- Priorizar el tipo de incidente.
- Diagnóstico del servicio.
- Validar el incidente y determinar si es posible darle solución.
- Cuando no es posible dar solución al incidente, realizar el correspondiente escalamiento a las áreas de soporte de segundo nivel.
- Realizar documentación de actividades realizadas.
- Realizar seguimiento, control y servicio solicitado.

A continuación se describe el proceso de soporte en la organización.

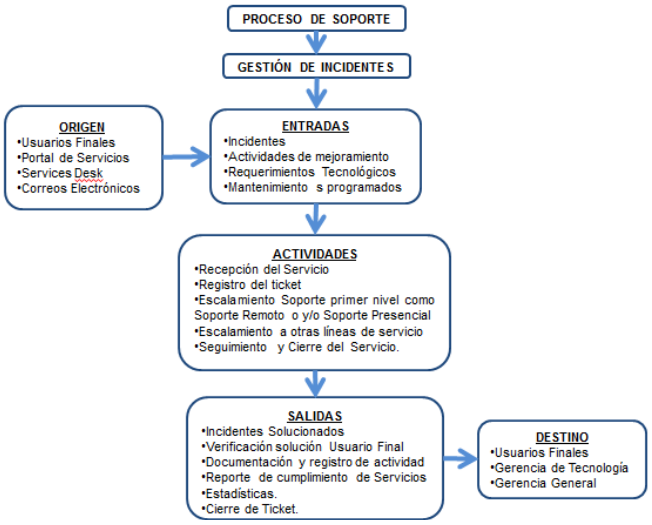


Figura 3. Proceso de Soporte de la Organización.
Fuente: autor.

El proceso de bases de datos es unos de los principales en el área de tecnología, este apoya a toda a la organización en que su operación no se detenga, ya que la operación de esta área es 24 horas al día.

Para identificar mejor el procedimiento de la administración de las bases de datos es necesario describir cada una de las actividades y procedimientos que conforman este proceso en la organización. También es necesario conocer que aunque no tiene los mismos niveles de servicio de soporte técnico, cumple la vital tarea de guardar toda la información de todos los sistemas de información.

TABLA II
PROCEDIMIENTO ADMINISTRACIÓN DE BASE DE DATOS

Procedimiento	Descripción
Administración en las bases de datos	Llevada a cabo por la persona encargada de definir y controlar las bases de datos corporativas que además proporciona asesorías a los desarrolladores, usuarios y ejecutivos que lo requieran.
Administración de la estructura de las bases de datos	Esta responsabilidad incluye participar en el diseño inicial de las bases de datos y su puesta en práctica, así como controlar y administrar sus requerimientos ayudando a evaluar alternativas.
Administración de las bases de datos	El DBA no es un usuario del sistema, no administra valores de datos sino la actividad de estos. Protege los datos, no los procesa.
Administrar el sistema manejador de las bases de datos	Este se encarga de seleccionar los estándares, así como la forma de la captura de la información y cómo es procesada y presentada.
Establecer diccionario de datos	Definir y estructurar cómo están configuradas las bases de datos para aquellos usuarios que tienen acceso.

Fuente: autor.

Los subprocesos más importantes de la organización frente a la administración y el manejo de la información se realizan a través de las bases de datos, estos son:

El subproceso número uno son las responsabilidades del administrador de bases de datos, esta es la persona que se encarga de la supervisión, administración y creación de las mismas y de los controles necesarios para apoyar las políticas, normas y procedimientos que tenga la organización.

En el subproceso número dos se describe la participación en el diseño inicial de las bases de datos y su puesta en práctica, así como controlar y administrar sus requerimientos.

En el subproceso número tres es de vital importancia saber qué modificaciones han sido efectuadas, cómo fueron realizadas y cuándo fueron establecidas. Una modificación sobre la estructura en la base de datos puede ocasionar un error a corto plazo.

E. Factores internos de la organización

Se conoce como el ambiente interno de la organización cada uno de los factores que se encuentran internamentamente interactuando con el fin de alcanzar sus objetivos de negocio a través del cumplimiento de sus políticas, cultura, estrategia y todo lo que se encuentre relacionado con el funcionamiento interno de la organización.

TABLA III
FACTORES INTERNOS DE LA ORGANIZACIÓN

Factor	Descripción
Personas	Personal técnico encargado del área de soporte.
Recursos tecnológicos	Equipos de cómputo y dispositivos de comunicaciones.
Procedimientos	Procedimientos definidos en el área de soporte para atención de incidentes.
Sistema de gestión de incidentes	Software para la gestión de incidentes.

Fuente: autor.

F. Factores externos de la organización.

Conjunto de circunstancias que pueden ocasionar el riesgo desde afuera de la organización.

TABLA IV
FACTORES EXTERNOS DE LA ORGANIZACIÓN

Factor	Descripción
Usuario final	Son las personas que realizan la solicitud del servicio a través del sistema de gestión.
Proveedores	Servicios que brindan apoyo en el proceso de soporte y permiten dar el cumplimento de los objetivos de la organización.
Económicos	Costos de inversión en el proceso de gestión de incidentes y adquisición de nuevas tecnologías.
Nuevas tecnologías	Actualizaciones en herramientas de hardware y software.

Fuente: autor.

En lo anterior identificamos las condiciones internas y externas del entorno de la organización, las cuales pueden generar oportunidades o eventos que afecten negativamente el cumplimiento de los objetivos.

G. Criterios de evaluación de probabilidad

A través de los criterios de evaluación de probabilidad identificamos qué tan probable pueden ocurrir cada uno de los riesgos de la organización.

TABLA V
CRITERIOS DE EVALUACIÓN DE PROBABILIDAD

Valor	Descriptor	Descripción
1	Casi certeza	Se espera que ocurra en la mayoría de las circunstancias.
2	Probable	Probablemente ocurrirá en la mayoría de las circunstancias.
3	Moderada	Ocurrirá en algún momento.
4	Improbable	Pudo ocurrir en algún momento.
5	Raro	Puede ocurrir en circunstancias excepcionales.

Fuente: autor.

H. Criterios de evaluación de impacto

Los criterios de evaluación de impacto se utilizan para medir el nivel de afectación y qué pueden llegar a causar en la organización.

TABLA VI
CRITERIOS DE EVALUACIÓN DE IMPACTO

Criterios de evaluación de impacto		
Valor	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias mínimas.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto.
3	Moderada	Si el hecho llegara a presentarse, tendría medianas consecuencias.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias.
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias.

Fuente: autor.

I. Identificación del riesgo

En el proceso de identificación del riesgo encontramos los siguientes riesgos que pueden afectar la operación y continuidad del negocio.

TABLA VII
RIESGOS EN EL PROCESO DE SOPORTE

Riesgos en el proceso de soporte	
Riesgo	Descripción
No registran incidentes en la herramienta de gestión	No existe historial de incidentes y registro de actividades en la herramienta.
Daños en el dispositivo del usuario durante el soporte.	Se pueden presentar daños durante el servicio de soporte técnico en el equipo del usuario.
Soporte conexión remota	Al realizar el soporte por conexión remota se puede transferir virus a los equipos.
Pérdida de información	La información del usuario está expuesta a pérdida o daños.
Robo de dispositivo del técnico o usuario	La pérdida de activos es un aspecto crítico porque pone en riesgo la información de sus clientes e información de la organización.

Fuente: autor.

TABLA VIII
RIESGO EN EL PROCESO DE ADMINISTRACIÓN DE BASES DE DATOS

Bases de datos	
Riesgo	Descripción
Cuentas temporales que no se eliminan y quedan activas	Existen cuentas que se crearon temporalmente y aún no han sido desactivadas.
No se realiza mantenimiento de logs	El incremento del tamaño de los logs ocasiona el exceso de almacenamiento en discos y puede afectar la operación.
No se realizan los backups de respaldo	No se realizan backups de respaldo sobre las bases de datos, activo primordial de la organización.
No existe política de seguridad	No existe documentación sobre los perfiles y procesos de la administración de bases de datos de la organización.
Más de dos cuentas de administrador	Puede ser vulnerable a pérdidas de información a través de usuarios con permisos autorizados o cuentas administradoras.

Fuente: autor.

J. Análisis del riesgo

Realizamos el análisis de consecuencias del riesgo de acuerdo con los riesgos identificados en el proceso de soporte, en caso de que puedan ocurrir dentro de la organización, se definen pérdidas económicas, reputación y el respectivo valor del riesgo.

TABLA IX
ANÁLISIS DEL RIESGO EN EL PROCESO DE SOPORTE

Id	Riesgo	Pérdidas Económicas	Incidente
R1	No registran incidentes en la herramienta de gestión	Hasta $1’000.000	No existe historial de incidentes y registro de actividades en la herramienta.
R2	Daños en el dispositivo del usuario durante el soporte.	Entre $500.000 a $1’000.000	Pérdida de la información.
R3	Soporte conexión remota	Entre 1’000.001 a $1’500.000	Conexiones no son visibles para el técnico.
R4	Pérdida de información	Entre $1’000.001 a $1’500.000	Pérdida de información de la organización y clientes.
R5	Robo de dispositivo al técnico o usuario	Mayores a $5’000.001	Pérdida de información crítica de los servicios de la organización.

Fuente: autor.

TABLA X
ANÁLISIS DEL RIESGO EN BASES DE DATOS

Id	Riesgo	Pérdidas económicas	Incidentes
R6	Cuentas temporales que no se eliminan y quedan activas	Hasta $1’000.000	No existe control sobre el acceso a las bases de datos.
R7	No se realiza mantenimiento de log	Entre $500.000 a $1’000.000	Incremento de tamaño de los log
R8	No se realizan los backups de respaldo	Entre 1’000.001 a $1’500.000	Conexiones no son visibles para el técnico.
R9	No existe política de seguridad	Entre $1’000.001 a $1’500.000	No existe un proceso para la administración de bases de datos
R10	Más de dos cuentas de administrador	Mayores a $5’000.001	Acceso a personas no autorizadas. Posible robo de información

Fuente: autor.

K. Análisis del riesgo

A través de la matriz de calor se realiza la evaluación de cada uno de los riesgos expuestos en las anteriores tablas, a continuación se muestra el tipo matriz que será utilizada para realizar la respectiva evaluación de cada uno de los riegos identificados.

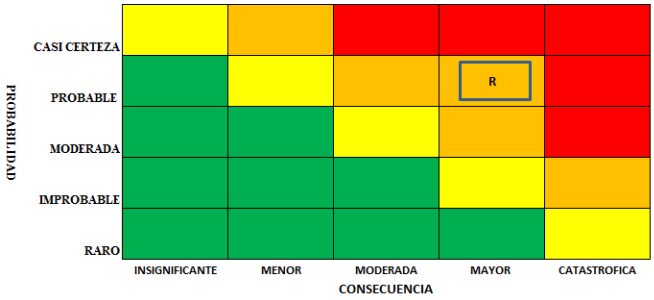


Figura 4. Matriz de calor, valoración de riesgos probabilidad vs consecuencias.
Fuente: autor.

Realizamos la evaluación de cada uno de los riesgos del servicio de soporte técnico.

La valoración del riesgo (R1) “no registro de incidente en la herramienta de gestión”, obtiene una calificación donde se determina que el riesgo es controlable y no tiene efectos negativos dentro de la organización.

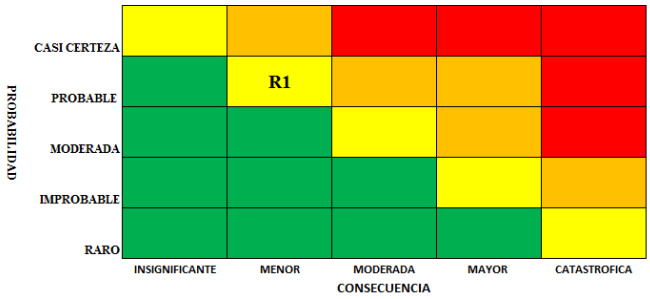


Figura 5. Matriz de calor, valoración del riesgo (R1) no registro de incidente en la herramienta de gestión.
Fuente: autor.

La valoración del riesgo (R2) “daños en el dispositivo del usuario durante el soporte”, obtiene una calificación donde se determina que el riesgo es improbable de materializar, pero generaría consecuencias moderadas en caso de llegar a presentarse.

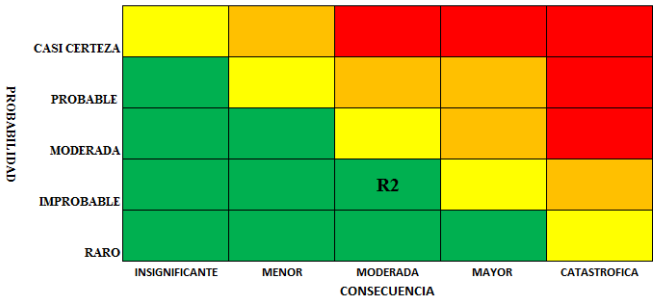


Figura 6. Matriz de calor, valoración del riesgo (R2) daños en el dispositivo del usuario durante el soporte.
Fuente: autor.

La valoración del riesgo (R3) “soporte conexión remota”, obtiene una calificación donde se determina que el riesgo es probable de materializar y tendría altas consecuencias en la organización.

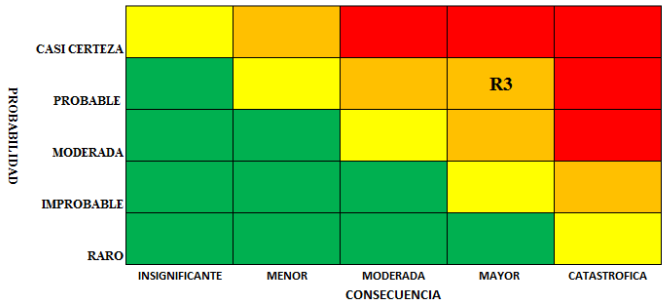


Figura 7. Matriz de calor, valoración del riesgo (R3) soporte conexión remota.
Fuente: autor.

La valoración del riesgo (R4) “pérdida de información”, obtiene una calificación donde se determina que el riesgo es probable de materializar y tendría altas consecuencias en la organización.

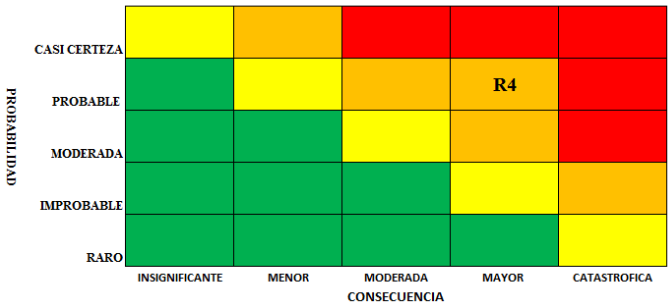


Figura 8. Matriz de calor, valoración del riesgo (R4) robo o pérdida de información.
Fuente: autor.

La valoración del riesgo (R5) "robo de dispositivo al técnico", obtiene una calificación donde se determina que el riesgo es probable de materializar y tendría consecuencias desastrosas en la imagen de la organización.

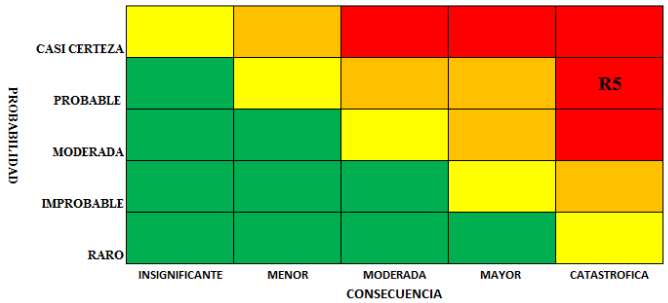


Figura 9. Matriz de calor, valoración del riesgo (R5) robo de dispositivo al técnico.
Fuente: autor.

A continuación, realizamos la evaluación de cada uno de los riesgos en los sistemas de bases de datos:

La valoración del riesgo (R6) "cuentas temporales que no se eliminan y quedan activas", obtiene una calificación donde se determina que el riesgo siempre sucede cuando se crean los usuarios en la base de datos y podría materializarse dependiendo de los perfiles de configuración.

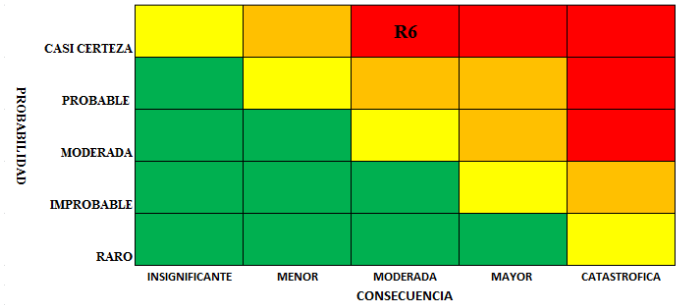


Figura 10. Matriz de calor, valoración del riesgo (R6) cuentas temporales o se eliminan y quedan activas.
Fuente: autor.

La valoración del riesgo (R7) "no se realiza mantenimiento de logs", obtiene una calificación donde se determina que el riesgo no es constante y no tiene una alta afectación en la organización.

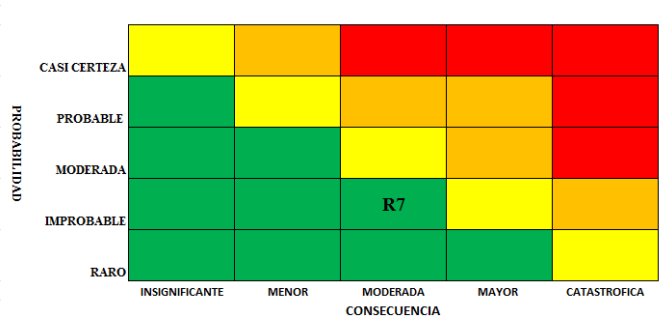


Figura 11. Matriz de calor, valoración del riesgo (R7) no se realiza mantenimiento de log.
Fuente: autor.

La valoración del riesgo (R8) "no se realiza los backups de respaldo", obtiene una calificación donde se determina que el riesgo es probable que suceda y puede tener un impacto medio dentro de la organización.

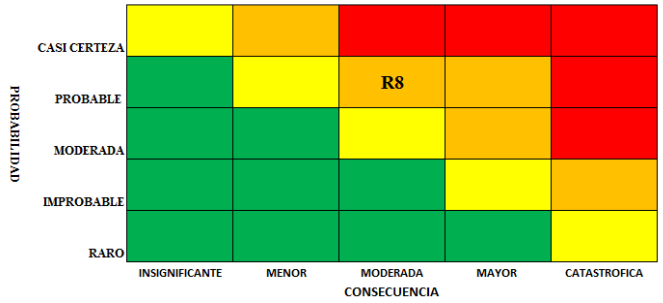


Figura 12. Matriz de calor, valoración del riesgo (R8) no se realiza los backups de respaldo.
Fuente: autor.

La valoración del riesgo (R9) "no existe política de seguridad", obtiene una calificación donde se determina que el riesgo es probable y puede tener una afectación alta dentro de la organización al no tener los procedimientos definidos para la administración de las bases de datos.

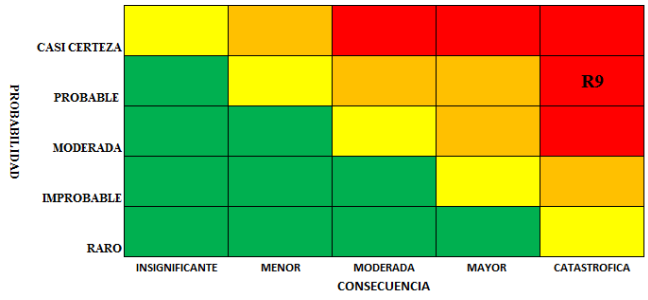


Figura 13. Matriz de calor, valoración del riesgo (R9) no existe política de seguridad.
Fuente: autor.

La valoración del riesgo (R10) "más de dos cuentas de administrador", obtiene una calificación donde se determina que el riesgo es probable y puede tener una afectación crítica y desastrosa para la organización.

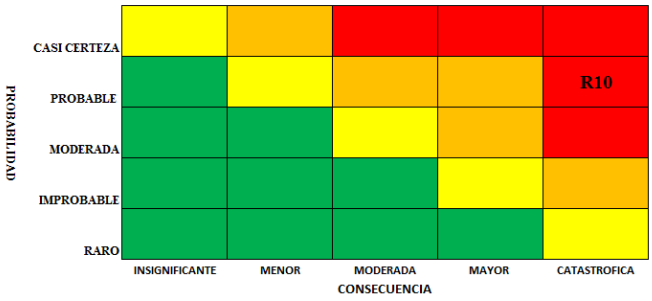


Figura 14. Matriz de calor, valoración del riesgo (R10) más de dos cuentas de administrador.
Fuente: autor.

L. Aplicación de controles

Por medio de la aplicación de controles entregamos las recomendaciones que puede aplicar la organización para la mitigación y control del riesgo.

TABLA XI
APLICACIÓN DE CONTROLES PROCESO DE SOPORTE

Id	Id Control	Control
R1	A.13.3.1	Registro de eventos y fallos. Descripción: realizar registros de fallas y eventos, crear procedimiento para el registro en la herramienta de gestión.
R2	A.11.2	Equipos. Descripción: Crear procedimientos para prevenir pérdida, daño o robo de dispositivos que interrumpa la operación de la organización.
R3	A.13.1.2	Seguridad de los servicios de red. Descripción: Identificar mecanismos de seguridad y niveles de servicios de red.
R4	A.12.3.1	Respaldo de la información. Descripción: Realizar copias de respaldo de la información, software de los sistemas de información.
R5	A.10.1	Controles criptográficos. Descripción: Implementar sistemas criptográficos en los equipos de la organización y garantizar confidencialidad, autenticidad y/o integridad de la información.

Fuente: autor.

TABLA XII
APLICACIÓN DE CONTROLES EN EL PROCESO DE ADMINISTRACIÓN DE BASES DE DATOS

Id	Id Control	Control
R6	A.9.2.1	Registro y cancelación de usuarios. Descripción: al existir cuentas que se crean temporalmente, tan pronto termine su vida útil deben ser inactivadas.
R7	A.12.1.13	Gestión de capacidad. Descripción: Realizar seguimiento a los recursos para asegurar su desempeño.
R8	A.13.1.2	Seguridad de los servicios de red. Descripción: Identificar mecanismos de seguridad y niveles de servicios de red.
R9	A.5.1.1	Política de la seguridad de la información. Descripción: Implantación de políticas y descripción del proceso de administración de bases de datos.
R10	A.9.2.3	Controles Criptográficos. Descripción: Restringir y controlar la asignación y uso de derechos de acceso privilegiados. Solo debe existir una cuenta de administración principal y una de respaldo con claves secretas y de uso controlado.

Fuente: autor.

REFERENCIAS

[1] 17799, E. I. (2005). *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.* ICONTEC.
[2] 73:2009, I. G. (2009). *Risk Management Vocabulary.* Bogota D.C.
[3] *ISO/IEC 31010, Risk Management. Risk Assessment Techniques.* (2009). BOGOTA D.C.: ISO.
[4] *Norma técnica colombiana NTC-ISO-27001: 2013.* (2013). Bogotá D.C : ICONTEC.

Oscar Fernando Jiménez Higuera, autor. Ingeniero de sistemas de la Universidad Piloto de Colombia Bogotá D.C. graduado en el año 2009.