ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA DE SISTEMAS

DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN EL ACOPLAMIENTO DE LA NORMA ISO/IEC 27005:2008 Y EL MÉTODO OCTAVE.

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE MÁSTER (Msc) EN CIENCIAS DE LA COMPUTACIÓN Y COMERCIO ELECTRÓNICO

WALTER GERMÁNICO CARRERA VILLAMARÍN

gpwsoft@gmail.com

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE MÁSTER (Msc) EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

SANTIAGO JAVIER GARCÍA VENEGAS

sjgarciav@gmail.com

DIRECTOR: ING. CARLOS MONTENEGRO

calos.montenegro@epn.edu.ec

Quito, Diciembre 2012

DECLARACIÓN

Yo, Walter Germánico Carrera Villamarín, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mi derecho de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Walter Germánico Carrera Villamarín

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Walter Germánico Carrera Villamarín, bajo mi supervisión.

Ing. Carlos Montenegro

DIRECTOR DE PROYECTO

DECLARACIÓN

Yo, Santiago Javier García Venegas, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mi derecho de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Santiago Javier García Venegas

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Santiago Javier García Venegas, bajo mi supervisión.

Ing. Carlos Montenegro

DIRECTOR DE PROYECTO

CONTENIDO

RESUMEN 1

PRESENTACIÓN 2

CAPÍTULO 1 4

GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN 4

1.1 NORMA ISO/IEC 27005:2008 4

1.1.1 ESTABLECIMIENTO DEL CONTEXTO 6

1.1.2 VALORACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN 6

1.1.3 TRATAMIENTO DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN 9

1.1.4 ACEPTACIÓN DEL RIESGO DE SEGURIDAD 10

1.1.5 COMUNICACIÓN DEL RIESGO DE SEGURIDAD 11

1.1.6 MONITOREO Y REVISIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN 11

1.2 OCTAVE 12

1.2.1 INTRODUCCIÓN AL MÉTODO OCTAVE 12

1.2.2 FASES DEL MÉTODO OCTAVE 13

1.2.2.1 La Preparación 13

1.2.2.2 Fase 1: Construir perfiles de amenaza basados en activos 14

1.2.2.3 Fase 2: Identificar las vulnerabilidades de la infraestructura 19

1.2.2.4 Fase 3: Desarrollar la estrategia y planes de seguridad 23

1.2.3 LA NATURALEZA NO LINEAL DEL MÉTODO OCTAVE 30

1.2.4 VARIACIONES EN EL MÉTODO OCTAVE 30

CAPÍTULO 2 31

DEFINICIÓN DEL ESQUEMA DE ACOPLAMIENTO DE LA NORMA ISO/IEC 27005:2008 CON EL MÉTODO OCTAVE 31

2.1 ESQUEMA METODOLÓGICO PARA EL ACOPLAMIENTO 31

2.2 ANÁLISIS COMPARATIVO DE LA NORMA ISO/IEC 27005:2008 CON EL MÉTODO OCTAVE 33

2.3 ANÁLISIS DE OPORTUNIDADES DE ACOPLAMIENTO DE COMPONENTES DE LA NORMA ISO/IEC 27005:2008 CON EL MÉTODO OCTAVE 40

2.4 ESQUEMA DE ACOPLAMIENTO DE LA NORMA ISO/IEC 27005:2008 CON EL MÉTODO OCTAVE 50

CAPÍTULO 3 60

DISEÑO DEL MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 60

3.1 INTRODUCCIÓN 60
3.1.1 ALCANCE 60
3.2 MARCO CONCEPTUAL 60
3.2.1 TAXONOMÍA DEL RIESGO 60
3.2.2 TÉRMINOS Y DEFINICIONES EN GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 64
3.3 ESTRUCTURA 68
3.3.1 ASPECTOS GENERALES 68
3.3.2 COMPONENTES ESTRUCTURALES 69
3.3.3 RECURSOS DOCUMENTALES ADICIONALES 72
3.4 DEFINICIÓN DE PROCESOS, ACTIVIDADES Y RECOMENDACIONES DE IMPLEMENTACIÓN 73
3.4.1 PROCESO DE INICIACIÓN 73
3.4.1.1 Actividad 1: Preparación 73
3.4.1.1.1 Detalle de actividad 73
3.4.1.1.2 Resultados 74
3.4.1.1.3 Recomendaciones de implementación 74
3.4.1.1.4 Fuentes 75
3.4.1.2 Actividad 2: Obtener patrocinio de la alta dirección 75
3.4.1.2.1 Detalle de actividad 75
3.4.1.2.2 Resultados 75
3.4.1.2.3 Recomendaciones de implementación 76
3.4.1.2.4 Fuentes 76
3.4.1.3 Actividad 3: Seleccionar a los miembros del equipo de análisis 76
3.4.1.3.1 Detalle de actividad 76
3.4.1.3.2 Resultados 76
3.4.1.3.3 Recomendaciones de implementación 77
3.4.1.3.4 Fuentes 77
3.4.2 PROCESO DE DEFINICIÓN DEL CONTEXTO ORGANIZACIONAL 77
3.4.2.1 Actividad 4: Definir el alcance 77
3.4.2.1.1 Detalle de actividad 77
3.4.2.1.2 Resultados 78
3.4.2.1.3 Recomendaciones de implementación 78
3.4.2.1.4 Fuentes 78

3.4.2.2 Actividad 5: Selección de los participantes 78
3.4.2.2.1 Detalle de actividad 78
3.4.2.2.2 Resultados 79
3.4.2.2.3 Recomendaciones de implementación 79
3.4.2.2.4 Fuentes 79
3.4.2.3 Actividad 6: Determinar la metodología de estimación de riesgo 79
3.4.2.3.1 Detalle de actividad 79
3.4.2.3.2 Resultados 81
3.4.2.3.3 Recomendaciones de implementación 81
3.4.2.3.4 Fuentes 84
3.4.2.4 Actividad 7: Definir el criterio básico de evaluación de riesgo 84
3.4.2.4.1 Detalle de actividad 84
3.4.2.4.2 Resultados 85
3.4.2.4.3 Recomendaciones de implementación 85
3.4.2.4.4 Fuentes 86
3.4.2.5 Actividad 8: Definir el criterio básico de impacto 86
3.4.2.5.1 Detalle de actividad 86
3.4.2.5.2 Resultados 87
3.4.2.5.3 Recomendaciones de implementación 87
3.4.2.5.4 Fuentes 88
3.4.2.6 Actividad 9: Definir el criterio básico de aceptación de riesgo 88
3.4.2.6.1 Detalle de actividad 88
3.4.2.6.2 Resultados 89
3.4.2.6.3 Recomendaciones 89
3.4.2.6.4 Fuentes 90
3.4.2.7 Actividad 10: Definir la organización para la gestión de riesgos de seguridad de la información 90
3.4.2.7.1 Detalle de actividad 90
3.4.2.7.2 Resultados 90
3.4.2.7.3 Recomendaciones de implementación 91
3.4.2.7.4 Fuentes 91
3.4.3 PROCESO DE IDENTIFICACIÓN DE RIESGOS 91
3.4.3.1 Actividad 11: Identificar activos 91
3.4.3.1.1 Detalle de actividad 91

3.4.3.1.2 Resultados 92
3.4.3.1.3 Recomendaciones de implementación 92
3.4.3.1.4 Fuentes 93
3.4.3.2 Actividad 12: Identificar las áreas de interés 93
3.4.3.2.1 Detalle de actividad 93
3.4.3.2.2 Resultados 93
3.4.3.2.3 Recomendaciones de implementación 94
3.4.3.2.4 Fuentes 95
3.4.3.3 Actividad 13: Identificar los requisitos de seguridad 95
3.4.3.3.1 Detalle de actividad 95
3.4.3.3.2 Resultados 95
3.4.3.3.3 Recomendaciones de implementación 96
3.4.3.3.4 Fuentes 97
3.4.3.4 Actividad 14: Identificar controles existentes 97
3.4.3.4.1 Detalle de actividad 97
3.4.3.4.2 Resultados 97
3.4.3.4.3 Recomendaciones de implementación 98
3.4.3.4.4 Fuentes 99
3.4.3.5 Actividad 15: Identificar amenazas 99
3.4.3.5.1 Detalle de actividad 99
3.4.3.5.2 Resultados 100
3.4.3.5.3 Recomendaciones de implementación 101
3.4.3.5.4 Fuentes 103
3.4.3.6 Actividad 16: Seleccionar los componentes de la infraestructura a evaluar 103
3.4.3.6.1 Detalle de actividad 103
3.4.3.6.2 Resultados 104
3.4.3.6.3 Recomendaciones de implementación 105
3.4.3.6.4 Fuentes 106
3.4.3.7 Actividad 17: Identificar vulnerabilidades tecnológicas 107
3.4.3.7.1 Detalle de actividad 107
3.4.3.7.2 Resultados 107
3.4.3.7.3 Recomendaciones de implementación 108
3.4.3.7.4 Fuentes 109

3.4.4 PROCESO DE EVALUACIÓN DE RIESGOS 109
3.4.4.1 Actividad 18: Identificar impacto 109
3.4.4.1.1 Detalle de actividad 109
3.4.4.1.2 Resultados 110
3.4.4.1.3 Recomendaciones de implementación 110
3.4.4.1.4 Fuentes 111
3.4.4.2 Actividad 19: Valorar el impacto de las amenazas 111
3.4.4.2.1 Detalle de actividad 111
3.4.4.2.2 Resultados 111
3.4.4.2.3 Recomendaciones de implementación 113
3.4.4.2.4 Fuentes 115
3.4.4.3 Actividad 20: Describir la probabilidad de amenazas 115
3.4.4.3.1 Detalle de actividad 115
3.4.4.3.2 Resultados 116
3.4.4.3.3 Recomendaciones de implementación 116
3.4.4.3.4 Fuentes 117
3.4.4.4 Actividad 21: Definir el criterio de probabilidad 117
3.4.4.4.1 Detalle de actividad 117
3.4.4.4.2 Resultados 117
3.4.4.4.3 Recomendaciones de implementación 118
3.4.4.4.4 Fuentes 118
3.4.4.5 Actividad 22: Valorar la probabilidad de incidente 118
3.4.4.5.1 Detalle de actividad 118
3.4.4.5.2 Resultados 119
3.4.4.5.3 Recomendaciones de implementación 119
3.4.4.5.4 Fuentes 120
3.4.4.6 Actividad 23: Estimar (valorar) y priorizar el nivel de riesgo 120
3.4.4.6.1 Detalle de actividad 120
3.4.4.6.2 Resultados 121
3.4.4.6.3 Recomendaciones de implementación 121
3.4.4.6.4 Fuentes 123
3.4.5 PROCESO DE TRATAMIENTO AL RIESGO 123
3.4.5.1 Actividad 24: Crear una estrategia de protección 124

3.4.5.1.1 Detalle de actividad 124
3.4.5.1.2 Resultados 124
3.4.5.1.3 Recomendaciones de implementación 125
3.4.5.1.4 Fuentes 126
3.4.5.2 Actividad 25: Crear planes de mitigación 126
3.4.5.2.1 Detalle de actividad 126
3.4.5.2.2 Resultados 128
3.4.5.2.3 Recomendaciones de implementación 129
3.4.5.2.4 Fuentes 129
3.4.5.3 Actividad 26: Crear lista de acciones 130
3.4.5.3.1 Detalle de actividad 130
3.4.5.3.2 Resultados 130
3.4.5.3.3 Recomendaciones de implementación 130
3.4.5.3.4 Fuentes 131
3.4.5.4 Actividad 27: Preparar la presentación de tratamiento al riesgo 131
3.4.5.4.1 Detalle de actividad 131
3.4.5.4.2 Resultados 131
3.4.5.4.3 Recomendaciones de implementación 132
3.4.5.4.4 Fuentes 132
3.4.5.5 Actividad 28: Crear los siguientes pasos 132
3.4.5.5.1 Detalle de actividad 132
3.4.5.5.2 *Resultados* 133
3.4.5.5.3 Recomendaciones de implementación 133
3.4.5.5.4 Fuentes 133
3.4.6 PROCESO DE COMUNICACIÓN DEL RIESGO 133
3.4.6.1 Actividad 29: Comunicar el riesgo 134
3.4.6.1.1 Detalle de actividad 134
3.4.6.1.2 Resultados 134
3.4.6.1.3 Recomendaciones de implementación 134
3.4.6.1.4 Fuentes 135
3.4.7 PROCESO DE MONITOREO Y REVISIÓN DEL RIESGO 135
3.4.7.1 Actividad 30: Monitorear y revisar los factores de riesgo 135
3.4.7.1.1 Detalle de actividad 135

3.4.7.1.2 Resultados 135
3.4.7.1.3 Recomendaciones de implementación 136
3.4.7.1.4 Fuentes 136
3.4.7.2 Actividad 31: Monitorear, revisar y mejorar de la gestión de riesgo 136
3.4.7.2.1 Detalle de actividad 136
3.4.7.2.2 Resultados 137
3.4.7.2.3 Recomendaciones de implementación 138
3.4.7.2.4 Fuentes 138
CAPÍTULO 4 139
APLICACIÓN AL CASO DE ESTUDIO 139
4.1 INTRODUCCIÓN 139
4.2 PROCEDIMIENTO 139
4.3 APLICACIÓN A LA EMPRESA ELÉCTRICA QUITO S.A. 140
4.3.1 CARACTERIZACIÓN DE LA EMPRESA ELÉCTRICA QUITO 140
4.3.1.1 Reseña histórica 140
4.3.1.2 Misión, Visión y Objetivos 141
4.3.1.3 Mapa de procesos 141
4.3.1.4 Unidad de TI y posición en la toma de decisiones 142
4.3.1.5 Organización para la gestión de riesgos de seguridad de la información y su posición 143
4.3.2 APLICACIÓN DEL MODELO 144
4.3.2.1 Proceso de Iniciación 144
4.3.2.1.1 Actividad 1: Preparación 144
4.3.2.1.2 Actividad 2: Obtener patrocinio de la alta dirección 147
4.3.2.1.3 Actividad 3: Seleccionar a los miembros del equipo de análisis 149
4.3.2.2 Proceso de definición del contexto organizacional 150
4.3.2.2.1 Actividad 4: Definir el alcance 150
4.3.2.2.2 Actividad 5: Selección de los participantes 151
4.3.2.2.3 Actividad 6: Determinar la metodología de estimación de riesgo 152
4.3.2.2.4 Actividad 7: Definir el criterio básico de evaluación de riesgo 153
4.3.2.2.5 Actividad 8: Definir el criterio básico de impacto 155
4.3.2.2.6 Actividad 9: Definir el criterio básico de aceptación de riesgo 157
4.3.2.2.7 Actividad 10: Definir la organización para la gestión de riesgos de seguridad de la información 158

4.3.2.3 Proceso de identificación de riesgos 159
4.3.2.3.1 Actividad 11: Identificar activos 159
4.3.2.3.2 Actividad 12: Identificar las áreas de interés 161
4.3.2.3.3 Actividad 13: Identificar los requisitos de seguridad 162
4.3.2.3.4 Actividad 14: Identificar controles existentes. 164
4.3.2.3.5 Actividad 15: Identificar amenazas 165
4.3.2.3.6 Actividades 16 y 17: Seleccionar los componentes de la infraestructura a evaluar e Identificar vulnerabilidades tecnológicas 167
4.3.2.4 Proceso de evaluación de riesgos 168
4.3.2.4.1 Actividad 18: Identificar impacto 168
4.3.2.4.2 Actividad 19: Valorar el impacto de las amenazas 169
4.3.2.4.3 Actividad 20: Describir la probabilidad de amenazas 172
4.3.2.4.4 Actividad 21: Definir el criterio de probabilidad 173
4.3.2.4.5 Actividad 22: Valorar la probabilidad de incidente 174
4.3.2.4.6 Actividad 23: Estimar (valorar) y priorizar el nivel de riesgo 175
4.3.2.5 Proceso de tratamiento al riesgo 177
4.3.2.5.1 *Actividad 24: Crear una estrategia de protección* 177
4.3.2.5.2 Actividad 25: Crear planes de mitigación 178
4.3.2.5.3 Actividad 26: Crear lista de acciones 181
4.3.2.5.4 Actividad 27: Preparar la presentación del tratamiento al riesgo 182
4.3.2.5.5 Actividad 28: Crear los siguientes pasos 183
4.3.2.6 Proceso de comunicación del riesgo 184
4.3.2.6.1 Actividad 29: Comunicar el riesgo 184
4.3.2.7 Proceso de monitoreo y revisión del riesgo 186
4.3.2.7.1 Actividad 30: Monitorear y revisar los factores de riesgo 186
4.3.2.7.2 Actividad 31: Monitorear, revisar y mejorar la gestión de riesgo 187
4.4 ANÁLISIS DE RESULTADOS 188
4.4.1 ASPECTOS GENERALES 188
4.4.2 ANÁLISIS DE RESULTADOS POR ACTIVIDAD 188
4.4.3 ANÁLISIS DE APLICABILIDAD TÉCNICA 190
4.4.4 ANÁLISIS DE APLICABILIDAD ECONÓMICA 192
4.4.5 ANÁLISIS DE APLICABILIDAD LEGAL 193
4.4.6 ANÁLISIS DE APLICABILIDAD OPERACIONAL 195
4.4.7 ANÁLISIS DE APLICABILIDAD DE CRONOGRAMA 195

CAPÍTULO 5 197
CONCLUSIONES Y RECOMENDACIONES 197
5.1 CONCLUSIONES 197
5.2 RECOMENDACIONES 202
REFERENCIAS BIBLIOGRÁFICAS 204
ANEXOS 205
ANEXO 1: NOMENCLATURA PARA COMPARATIVA NORMA ISO/IEC 27005:2008, MÉTODO OCTAVE. 205
ANEXO 2: DESCRIPCIONES COMPARATIVAS DETALLADAS DE LA NORMA ISO/IEC 27005:2008 Y EL MÉTODO OCTAVE. 205
ANEXO 3: OPORTUNIDADES DE ACOPLAMIENTO ENTRE LA NORMA ISO/IEC 27005:2008 Y EL MÉTODO OCTAVE. 205
ANEXO 4: PERFIL GENÉRICO DE RIESGOS. 205
ANEXO 5: PERFIL GENÉRICO DE RIESGOS PARA EEQ. 205
ANEXO 6: PLANTILLAS. 205
ANEXO 7: RESULTADOS. 205

Índice de Tablas

Tabla 1.1-1: Componentes del establecimiento del contexto 6
Tabla 1.1-2: Actividades de la valoración del riesgo de seguridad de la información 9
Tabla 1.1-3: Opciones de tratamiento al riesgo 10
Tabla 1.1-4: Actividades de monitoreo y revisión de riesgo de seguridad de la información 11
Tabla 1.2-1: Criterios y método OCTAVE 12
Tabla 1.2-2: Atributos y los resultados del enfoque de OCTAVE 13
Tabla 1.2-3: Actividades para la preparación del método OCTAVE 14
Tabla 1.2-4: Fase 1 del método OCTAVE, construir perfiles de amenaza basados en activos 16
Tabla 1.2-5: Categorización de amenazas 17
Tabla 1.2-6: Requerimientos de seguridad de la información 18
Tabla 1.2-7: Categorías de amenaza por tipos de activo 18
Tabla 1.2-8: Ejemplo de árbol de amenaza 19
Tabla 1.2-9: Categorización de vulnerabilidades 20
Tabla 1.2-10: Áreas de práctica operacional 20
Tabla 1.2-11: Fase 2 del método OCTAVE, Identificar las vulnerabilidades de la infraestructura 21
Tabla 1.2-12: Categorización de activos vs Sistemas de interés 21
Tabla 1.2-13Ejemplo de clases de componentes claves a evaluar 22
Tabla 1.2-14: Fase 3 del método OCTAVE, Desarrollar la estrategia y planes de seguridad 25
Tabla 1.2-15: Ejemplo de descripción de impacto por activo 26
Tabla 1.2-16: Ejemplo de criterio de evaluación por área de impacto 26
Tabla 1.2-17: Ejemplo de criterio de probabilidad 27
Tabla 1.2-18: Ejemplo de perfil de riesgo con probabilidad e impacto 27
Tabla 1.2-19: Ejemplo de consolidación de información de procesos 1-3 28
Tabla 1.2-20: Ejemplo de estrategia de protección 28
Tabla 1.2-21: Ejemplo de perfil de riesgo con enfoque y plan de mitigación 29
Tabla 1.2-22: Matriz de valor 29
Tabla 1.2-23: Ejemplo de perfil de riesgo considerando el valor esperado 30
Tabla 2.1-1: Comparativa inicial de la norma ISO/IEC 27005:2008 y el método OCTAVE 32
Tabla 2.2-1 Descripciones comparativas detalladas de la norma ISO/IEC 27005:2008 y el método OCTAVE 39
Tabla 2.3-1 Oportunidades de acoplamiento entre la norma ISO/IEC 27005:2008 y el método OCTAVE 50
Tabla 2.4-1 Esquema de acoplamiento de la norma ISO/IEC 27005:2008 con el Método OCTAVE 54
Tabla 2.4-2Principios y atributos del enfoque OCTAVE 58
Tabla 2.4-3 Cantidad de actividades por modelo para el esquema de acoplamiento 59

Tabla 3.4-1 Matriz de valor esperado (enfoque cualitativo) 82
Tabla 3.4-2 Matriz de estimación de riesgo (enfoque cuantitativo) 83
Tabla 3.4-3 Matriz de valor esperado (enfoque cuantitativo) 84
Tabla 3.4-4 Ejemplo de criterio de evaluación de riesgo 86
Tabla 3.4-5 Ejemplo de priorización de áreas de impacto 87
Tabla 3.4-6 Ejemplo de criterio básico de impacto 88
Tabla 3.4-7 Ejemplo de criterio básico de aceptación de riesgo 89
Tabla 3.4-8 Ejemplo de matriz de identificación de activos 93
Tabla 3.4-9 Fuentes de amenaza vs Resultados 94
Tabla 3.4-10 Ejemplo de áreas de interés vs resultados vs Impacto por activo 95
Tabla 3.4-11 Ejemplo de requisitos de seguridad por activo 96
Tabla 3.4-12 Ejemplo de áreas de interés mapeadas a propiedades de amenaza 101
Tabla 3.4-13 Requerimientos de seguridad vs resultados 102
Tabla 3.4-14 Tipos de activo vs Categorías de amenaza aplicables 103
Tabla 3.4-15 Categorías de activo vs Áreas de interés 105
Tabla 3.4-16 Ejemplo de razones de selección por clase de componente clave 105
Tabla 3.4-17 Ejemplo de lista de componentes de infraestructura a evaluar 106
Tabla 3.4-18 Ejemplo de evaluación de vulnerabilidades tecnológicas 108
Tabla 3.4-19 Ejemplo de resumen de resultados de evaluación de vulnerabilidades tecnológicas 108
Tabla 3.4-20 Ejemplo de descripción de impacto por resultado y activo. 111
Tabla 3.4-21 Ejemplo de valoración de impacto por activo y resultado 114
Tabla 3.4-22 Ejemplo de asignación de descripciones de probabilidad de impacto 117
Tabla 3.4-23 Ejemplo de criterio de probabilidad 118
Tabla 3.4-24 Matriz de valor esperado 122
Tabla 3.4-25 Ejemplo de enfoques estratégicos de tratamiento al riesgo 125
Tabla 3.4-26 Ejemplo de lista de acciones 131
Tabla 4.4-1 Análisis de resultados 189
Tabla 4.4-2 Costos de personal 192
Tabla 4.4-3 Costos de equipos y suministros 193

Índice de Figuras

Figura 1.1-1 Proceso de gestión de riesgos de seguridad de la información 5
Figura 1.1-2 Actividades del tratamiento al riesgo. 9
Figura 2.1-1 Esquema de acoplamiento 33
Figura 2.4-1 Distribución porcentual de actividades fuera/dentro de esquema de acoplamiento por modelo 59
Figura 3.2-1 Taxonomía del riesgo 61
Figura 3.3-1 Modelo de gestión de riesgos de seguridad de la información 70
Figura 3.4-1 Ejemplo de árbol de amenaza con áreas de interés 101
Figura 3.4-2 Ejemplo de perfil de riesgo 115
Figura 3.4-3 Ejemplo de perfil de riesgo con probabilidad e impacto valorados 120
Figura 3.4-4 Ejemplo de perfil de riesgo con estimación de riesgo y prioridad 122
Figura 3.4-5 Ejemplo de perfil de riesgo con planes de mitigación y lista de acciones ... 129
Figura 4.3-1 Mapa de procesos EEQ 142
Figura 4.3-2 Estructura Orgánica de la Empresa Eléctrica Quito 143
Figura 4.3-3 Orgánico estructural de la Dirección de tecnología de información y comunicaciones 144
Figura 4.4-1 Diagrama Gantt por procesos 196

Índice de Plantillas

Plantilla 3.4-1 Actividades de preparación 74
Plantilla 3.4-2 Patrocinio de la alta dirección 75
Plantilla 3.4-3 Selección de miembros del equipo de análisis 77
Plantilla 3.4-4 Definición del alcance 78
Plantilla 3.4-5 Selección de participantes 79
Plantilla 3.4-6 Determinar la metodología de estimación del riesgo 81
Plantilla 3.4-7 Definición de criterio básico de evaluación de riesgo 85
Plantilla 3.4-8 Definición de criterio básico de impacto 87
Plantilla 3.4-9 Criterio básico de aceptación del riesgo 89
Plantilla 3.4-10 Definición de la organización de gestión de riesgos de seguridad de la información 90
Plantilla 3.4-11 Identificación de activos 92
Plantilla 3.4-12 Identificar áreas de interés 94
Plantilla 3.4-13 Requisitos de seguridad 96
Plantilla 3.4-14 Definición de controles existentes 98
Plantilla 3.4-15 Identificar Amenazas 100
Plantilla 3.4-16 Árbol de amenaza 100
Plantilla 3.4-17 Clases de componentes de infraestructura a evaluar 104
Plantilla 3.4-18 Componentes de infraestructura a evaluar 104
Plantilla 3.4-19 Identificar vulnerabilidades 107
Plantilla 3.4-20 Identificar Impacto 110
Plantilla 3.4-21 Valorar impacto 112
Plantilla 3.4-22 Perfil de riesgo 112
Plantilla 3.4-23 Describir probabilidad de amenaza 116
Plantilla 3.4-24 Definir criterio de probabilidad 117
Plantilla 3.4-25 Criterio de probabilidad individual 118
Plantilla 3.4-26 Perfil de riesgo con probabilidad e impacto 119
Plantilla 3.4-27 Perfil de riesgo con riesgo estimado y prioridad 121
Plantilla 3.4-28 Definición de estrategia de protección 125
Plantilla 3.4-29 Perfil de riesgo con planes de mitigación y acciones 128
Plantilla 3.4-30 Crear acciones 130
Plantilla 3.4-31 Presentación de tratamiento del riesgo 131
Plantilla 3.4-32 Crear los siguientes pasos 133
Plantilla 3.4-33 Plan de comunicación 134
Plantilla 3.4-34 Monitorear y revisar factores de riesgo 136
Plantilla 3.4-35 Monitorear, revisar y mejorar la gestión de riesgos 138

Índice de Resultados

Resultado 4.3-1 Actividades de preparación 145
Resultado 4.3-2 Diagrama Gantt (cronograma) 146
Resultado 4.3-3 Patrocinio de la alta dirección 148
Resultado 4.3-4 Selección de miembros del equipo de análisis 149
Resultado 4.3-5 Definición del alcance 150
Resultado 4.3-6 Selección de participantes 151
Resultado 4.3-7 Determinar la metodología de estimación del riesgo 152
Resultado 4.3-8 Definición de criterio básico de evaluación de riesgo 154
Resultado 4.3-9 Definición de criterio básico de impacto 156
Resultado 4.3-10 Criterio básico de aceptación del riesgo 157
Resultado 4.3-11 Definición de la organización de gestión de riesgos de seguridad de la información 159
Resultado 4.3-12 Identificación de activos 160
Resultado 4.3-13 Activos críticos 160
Resultado 4.3-14 Identificar áreas de interés 161
Resultado 4.3-15 Requisitos de seguridad 163
Resultado 4.3-16 Resumen de controles existentes 164
Resultado 4.3-17 Identificar Amenazas 166
Resultado 4.3-18 Árbol de amenaza Sieeq Comercial (acceso Red) 166
Resultado 4.3-19 Identificar Impacto Sieeq Comercial 169
Resultado 4.3-20 Impacto valorado Sieeq Comercial 170
Resultado 4.3-21 Perfil de riesgo Sieeq Comercial (acceso red) 171
Resultado 4.3-22 Describir probabilidad de amenaza Sieeq Comercial 172
Resultado 4.3-23 Definir criterio de probabilidad 173
Resultado 4.3-24 Perfil de riesgo con probabilidad e impacto, Sieeq Comercial (acceso red) 174
Resultado 4.3-25 Perfil de riesgo con riesgo estimado y prioridad, Sieeq Comercial (acceso red) 176
Resultado 4.3-26 Riesgos altos 176
Resultado 4.3-27 Definición de estrategia de protección 178
Resultado 4.3-28 Perfil de riesgo con planes de mitigación y acciones, Sieeq Comercial (acceso red) 180
Resultado 4.3-29 Crear acciones 181
Resultado 4.3-30 Presentación de tratamiento del riesgo 182
Resultado 4.3-31 Crear los siguientes pasos 184
Resultado 4.3-32 Plan de comunicación 185

RESUMEN

El presente trabajo muestra un marco conceptual de referencia que incluye un análisis relacionado a la norma ISO/IEC 27005:2008 y el método OCTAVE, con esta base se procede a establecer las oportunidades de acoplamiento entre estos dos esquemas, con el objetivo de definir un modelo de gestión de riesgos de seguridad de la información. A continuación se aplica el modelo propuesto a un caso de estudio práctico, para posteriormente validar su aplicabilidad en los ámbitos técnico, económico, legal, organizacional y de cronograma. Finalmente se establecen las conclusiones y recomendaciones.

PRESENTACIÓN

La información, al igual que cualquier otro activo importante de una organización, necesita ser protegida adecuadamente. Cualquiera que sea la forma en que la información pueda presentarse, con el objetivo de protegerla, es necesario garantizar su confidencialidad, integridad y disponibilidad. Una de las formas de solucionar la problemática de seguridad de la información, es la gestión de riesgos de seguridad de la información.

El presente proyecto de tesis va orientado a presentar una propuesta de un modelo de gestión de riesgos de seguridad de la información que pretende establecer los procesos y actividades que le permitirían a una organización gestionar sus riesgos de seguridad de la información.

La tesis se compone en cinco capítulos organizados de tal manera que permitan generar una guía clara y práctica de cómo generar y validar la aplicabilidad de un modelo de gestión de riesgos de seguridad de la información basado en el acoplamiento de la norma ISO/IEC 27005:2008 y el método OCTAVE.

En el capítulo 1 se establece un marco conceptual de referencia en base al análisis de los lineamientos de gestión de riesgos de seguridad de la información propuestos por la norma ISO/IEC 27005:2008 y las actividades sistemáticas para evaluación y planificación estratégica de riesgos de seguridad de la información propuestas por el método OCTAVE.

En el capítulo 2, se define el esquema de acoplamiento de la norma ISO/IEC 27005:2008 y el método OCTAVE, en base al análisis de oportunidades de acoplamiento de las actividades propuestas por ambos esquemas. Se toma como referencia principal las actividades propuestas por la norma ISO/IEC 27005:2008 debido a que esta propuesta es un estándar y adicionalmente a que es más actual que el método OCTAVE. El esquema incluye todas las actividades de la norma

ISO/IEC 27005:2008 e incluye varias actividades del método OCTAVE, con el objetivo de fortalecer el modelo.

En el capítulo 3, se define los procesos y actividades del modelo de gestión de riesgos de seguridad propuesto, en base al esquema de acoplamiento definido en el capítulo 2. Para el efecto, se realizó un refinamiento a cada actividad, con el objetivo de estandarizar aspectos como la terminología y documentación referencial como catálogo de prácticas, amenazas y vulnerabilidades. Se incluyó recomendaciones de implementación y plantillas de ayuda a ser llenadas en la implementación.

En el capítulo 4, se desarrolló la aplicación del modelo de gestión de riesgos de seguridad de la información propuesto a un caso de estudio práctico, se incluye la caracterización de la organización seleccionada para el efecto. Se aplicó las actividades del modelo, registrando los resultados de cada una de ellas. Posteriormente se efectuó un análisis de los resultados obtenidos en comparación de los resultados esperados. A continuación, se realizó un análisis de aplicabilidad en los contextos técnico, económico, legal, operacional, organizacional y de cronograma.

Finalmente, en el capítulo 5, se estableció las conclusiones y recomendaciones.

CAPÍTULO 1
GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad de la información es el proceso de identificar riesgos e implementar planes para hacerles frente [1 pág. G5]. Existen normas, métodos y conjuntos de buenas prácticas que proveen lineamientos para ejecutar actividades enfocadas a la gestión de riesgos de seguridad de la información. En este capítulo se revisará dos de ellas, la norma ISO/IEC 27005:2008 y el método OCTAVE.

La norma ISO/IEC 27005:2008, provee lineamientos para la gestión de riesgos de seguridad de la información en una organización, dando soporte en particular a los requerimientos de un SGSI de acuerdo a la norma ISO/IEC 27001. Sin embargo, no provee una metodología específica de gestión de riesgos de seguridad de la información. Le corresponde a la organización definir su enfoque a la gestión de riesgos dependiendo por ejemplo del alcance de un SGSI, el contexto de la gestión de riesgos o sector de la industria [2 pág. VI].

OCTAVE, es una suite de herramientas, técnicas y métodos para evaluación y planificación estratégica de riesgos de seguridad de la información [3].

1.1 NORMA ISO/IEC 27005:2008

Para la norma ISO/IEC 27005:2008, el proceso de gestión de riesgos de seguridad de la información, consiste en los puntos señalados en la gráfica siguiente:

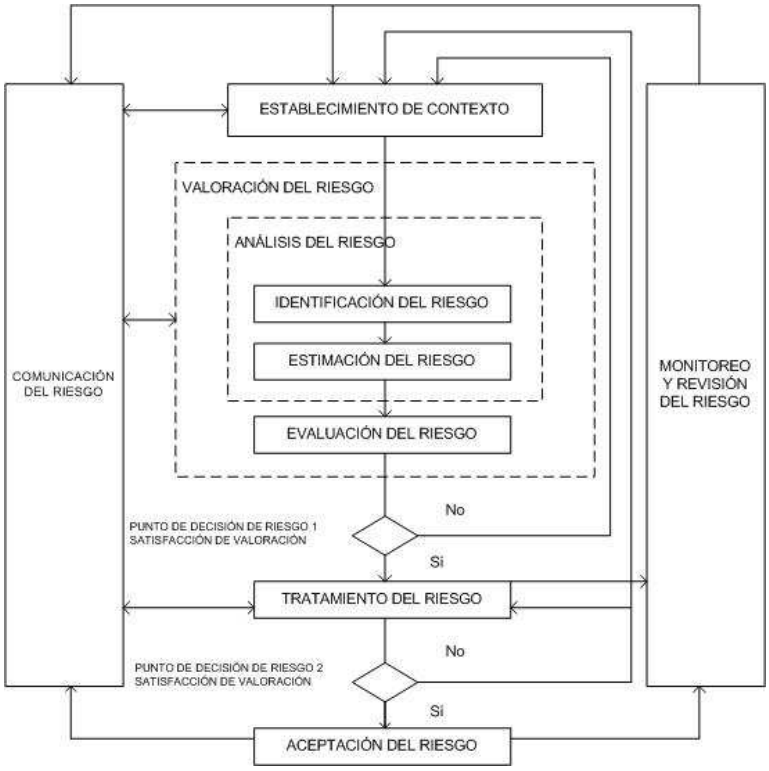


Figura 1.1-1 Proceso de gestión de riesgos de seguridad de la información

Fuente: Norma ISO 27005:2008

En la figura anterior, se puede ver como el proceso de gestión de riesgos de la seguridad de la información inicia con el establecimiento del contexto, seguido de la valoración del riesgo, que incluye la identificación, estimación y evaluación del riesgo. Posteriormente hay un punto de decisión donde se determina si hay suficiente información para determinar las acciones requeridas para modificar los riesgos a un nivel aceptable para luego completar el tratamiento del riesgo; si no hay información suficiente se debe realizar otra iteración, regresando al establecimiento del contexto. Cuando el tratamiento del riesgo no ha sido efectivo, es posible que no se obtenga un nivel de riesgo residual aceptable, entonces será necesaria otra iteración hacia el establecimiento del contexto.

La aceptación del riesgo debe ser explícita por parte de la alta directiva de la organización. Durante todo el proceso de la gestión de riesgos de seguridad de la

información, es necesario que los riesgos y su tratamiento sean comunicados a la alta directiva y al personal operacional adecuado.

1.1.1 ESTABLECIMIENTO DEL CONTEXTO

A continuación, se muestra el detalle de componentes del establecimiento del contexto:

Componente	**Actividad (definiciones)**	**Fuente**
Criterio básico	Criterio básico de evaluación del riesgo.	Información relevante de la organización.
	Criterio básico de impacto.	
	Criterio básico de aceptación del riesgo.	
Alcance y límites	Alcance.	
	Límites.	
Organización para la gestión de riesgos de seguridad de la información	Los roles y responsabilidades de esta organización incluye el desarrollo de procesos adecuados de la gestión de riesgos, la identificación y análisis de los interesados, la definición de roles y responsabilidades internas y externas, establecimiento de las relaciones entre la organización e interesados, interfaces hacia los más altos niveles de funciones de gestión de riesgos.	

Tabla 1.1-1: Componentes del establecimiento del contexto

Fuente: Los autores

1.1.2 VALORACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Cada organización puede utilizar su propio enfoque de valoración de riesgo, basado en los objetivos y metas de esta valoración, si se obtiene insuficiente información para evaluar el riesgo, se realiza un mayor análisis incluso considerando utilizar otro método. A continuación, se muestra el detalle de las actividades de la valoración del riesgo:

Componente	**Actividad**	**Fuente**

Componente	Actividad	Fuente
Identificación del riesgo	Incluye la identificación de activos dentro del alcance y su relación con los respectivos procesos del negocio. Un activo es cualquier cosa que pueda tener valor para la organización y que por consiguiente requiere protección [2 pág. 10].	Establecimiento del contexto
	Incluye la identificación de amenazas, su tipo y origen. Una amenaza tiene el potencial de causar daño a activos como información, procesos y sistemas, por tanto a organizaciones; las amenazas pueden tener un origen natural o humano y pueden ser accidentales o deliberadas, además pueden ser disparadas desde dentro o fuera de la organización [2 pág. 11].	Catálogo de amenazas, revisión de incidentes, dueños de activos.
	Incluye la identificación de controles existentes. Los controles se implementan de acuerdo a los planes de tratamiento del riesgo, la efectividad de un control se mide al verificar como reduce la probabilidad de ocurrencia de la amenaza, la facilidad de explotar una vulnerabilidad o el impacto de un incidente.	Documentación de controles, revisiones físicas en sitio y resultados de auditorías internas
	Incluye la identificación de vulnerabilidades, deben estar asociadas a los activos, amenazas y controles, sin embargo pueden existir vulnerabilidades que no se relacionan a alguna amenaza identificada. Las vulnerabilidades a ser identificadas son aquellas que pueden ser explotadas por amenazas para causar daño a los activos o a la organización.	Las áreas de identificación de amenazas son: procesos, personal, ambiente físico, configuración de sistemas de información

Componente	Actividad	Fuente
		(HW, SW y comunicaciones)
	Incluye la identificación de consecuencias que provocan perdida de confidencialidad, integridad y disponibilidad. Se forma de los escenarios con sus consecuencias relacionadas a los activos y procesos del negocio. Un escenario de incidente es una descripción de una amenaza explotando a una vulnerabilidad o un conjunto de ellas [2 pág. 13].	Listado de activos, procesos, amenazas, vulnerabilidades.
Estimación del riesgo	Una metodología de estimación de riesgo puede ser cualitativa, cuantitativa o una combinación, debe ser consistente con el criterio de evaluación del riesgo.	Datos históricos, criterio de evaluación de riesgo.
	Generar el listado de consecuencias (impacto para el negocio) valoradas de un escenario de incidente expresado respecto a los activos y criterio de impacto. Se debe empezar por clasificar los activos de acuerdo a su criticidad en alcanzar los objetivos de negocio, posteriormente se valora el activo, midiendo el valor de reemplazar el activo y la consecuencia para el negocio de la pérdida o comprometimiento del activo (como pérdidas por revelación, modificación, pérdida, interrupción).	Escenarios de incidentes, incluyendo amenazas, vulnerabilidades, activos afectados, consecuencias y procesos de negocio
	Generar la valoración cuantitativa o cualitativa de la probabilidad de incidente. Para cada escenario se requiere valorar la probabilidad e impacto, tomando en cuenta cuan a menudo la amenaza ocurre y cuan fácilmente las vulnerabilidades	Lista de escenarios de incidentes relevantes, lista de controles

Componente	Actividad	Fuente
	pueden ser explotadas.	existentes y planeados, su efectividad y estado de uso
	Determinar el nivel de estimación del riesgo en base a los valores a la probabilidad y consecuencia del riesgo.	Lista de escenarios de incidentes con su probabilidad.
Evaluación del riesgo	Determinar el conjunto de riesgos priorizados de acuerdo al criterio de evaluación de riesgo en relación con los escenarios de incidentes que condujeron a esos riesgos.	Análisis de riesgo

Tabla 1.1-2: Actividades de la valoración del riesgo de seguridad de la información

Fuente: Los autores

1.1.3 TRATAMIENTO DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

El propósito de este tratamiento es determinar controles para reducir, retener, evitar o transferir los riesgos a través de la definición de un plan de tratamiento al riesgo. La gráfica siguiente describe este proceso:

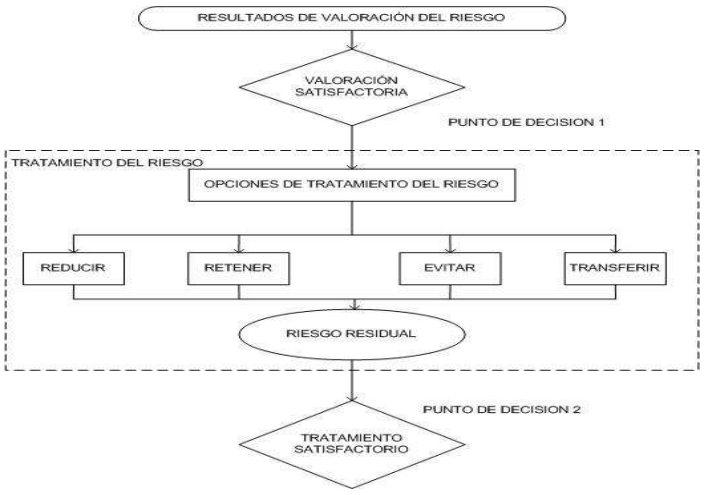


Figura 1.1-2 Actividades del tratamiento al riesgo.

Fuente: Norma ISO/IEC 27005:2008

Se debe elegir grandes reducciones del riesgo con poco gasto, las elecciones costosas deben ser justificadas.

Una vez definido el tratamiento del riesgo, se debe definir el riesgo residual, esto puede requerir una iteración sobre la valoración del riesgo dependiendo de los efectos esperados del tratamiento. En caso de que el riesgo residual no sea aceptado, se requerirá una nueva iteración del tratamiento del riesgo.

A continuación se muestran las opciones de tratamiento al riesgo:

Opción	**Actividad (descripción de opción de tratamiento)**
Reducción del riesgo	El nivel del riesgo puede ser reducido a través de la selección de controles, de tal forma que el riesgo residual pueda ser re valorizado hasta ser aceptable.
Retención del riesgo	Retener el riesgo sin ninguna acción adicional, en base a la evaluación del riesgo. No hay necesidad de implementar controles adicionales si el nivel del riesgo satisface el criterio de aceptación.
Evitar los riesgos	Si los riesgos son muy altos o los costos de implementación de tratamiento son mayores a los beneficios, se puede evitar el riesgo mediante el retiro de una o varias actividades existentes o planificadas, o cambiando las condiciones sobre las cuales opera la actividad.
Transferencia de riesgos	Transferir los riesgos para que puedan ser gestionados más efectivamente, dependiendo de la evaluación del riesgo.

Tabla 1.1-3: Opciones de tratamiento al riesgo

Fuente: Los autores

1.1.4 ACEPTACIÓN DEL RIESGO DE SEGURIDAD

Para determinar la aceptación del riesgo, es necesario el plan de tratamiento del riesgo y el riesgo residual, en base a esto, la directiva organizacional debe decidir que riesgos son aceptados con la correspondiente justificación para aquellos casos que no satisfagan el criterio de aceptación normal del riesgo. En los casos en que el

riesgo es aceptado por ejemplo por que el costo de reducción es muy alto, se debería revisar el criterio de aceptación pues sería inadecuado.

1.1.5 COMUNICACIÓN DEL RIESGO DE SEGURIDAD

Toda información obtenida en las fases de la gestión del riesgo como la existencia, naturaleza, forma, probabilidad, severidad, tratamiento y aceptación del riesgo debe ser compartida con los interesados y otros entes de toma de decisiones, obteniendo así un continuo entendimiento del proceso de gestión de riesgos y sus resultados, de esta forma se puede alcanzar un acuerdo de cómo gestionar los riesgos. Los interesados hacen valoraciones acerca de la aceptabilidad del riesgo de acuerdo a su percepción del riesgo y del beneficio, y esta percepción varía, por lo que la percepción debe ser documentada.

1.1.6 MONITOREO Y REVISIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Este monitoreo y revisión, incluye los siguientes componentes:

Monitoreo	Descripción de actividad	Fuente
Monitoreo y revisión de factores de riesgo	Los riesgos no son estáticos, sus factores varían en el tiempo, que incluye cambios de las amenazas, probabilidad, consecuencias, valor de los activos, manteniendo un monitoreo y revisión continuo, se puede mantener una imagen general del riesgo.	Información de las actividades de gestión del riesgo.
Monitoreo, revisión y mejora de la gestión de riesgo	Permite asegurar que el contexto, valoración, tratamiento, planes son apropiados para la circunstancia. Toda mejora sobre los procesos debe ser notificada a los respectivos administradores para asegurarse que el riesgo no está siendo desestimado o pasado por alto.	Información de las actividades de gestión del riesgo.

Tabla 1.1-4: Actividades de monitoreo y revisión de riesgo de seguridad de la información

Fuente: Los autores

1.2 OCTAVE

OCTAVE analiza e identifica aquello que necesita ser protegido en la organización, determina porque es un riesgo y desarrolla soluciones con prácticas y tecnología. OCTAVE presenta los siguientes conceptos principales:

Criterios de OCTAVE	Principios, atributos y resultados que definen el enfoque OCTAVE para evaluaciones de riesgos de seguridad de la información.
Método OCTAVE	Indica como el enfoque OCTAVE puede implementarse en diferentes tipos de organización.

Tabla 1.2-1: Criterios y método OCTAVE

Fuente: Los autores

1.2.1 INTRODUCCIÓN AL MÉTODO OCTAVE

El Método OCTAVE utiliza un enfoque de tres fases (que parten de las fases de evaluación de seguridad propuestas por el enfoque OCTAVE) implementadas a través de talleres para el examen de las cuestiones de organización y tecnología, consta de varios procesos y además varias actividades de preparación deben ser completadas antes de la evaluación real.

Los atributos y los resultados del enfoque de OCTAVE:

Fases del Método OCTAVE	**Procesos por fase**	**Serie progresiva de talleres**
Preparación (se refiere a los factores críticos de éxito) Obtener patrocinio de la alta dirección para OCTAVE. Seleccionar a los miembros del equipo de análisis. Seleccionar las áreas operativas para que participen en OCTAVE (alcance). Selección de los participantes.		Los talleres tienen un líder y un documentador, no siempre se va tener el mismo líder o documentador para todos los talleres. El líder es responsable de dirigir todas las actividades del taller y garantiza que todos ellos se han completado, también es responsable de asegurar que todos los participantes

Coordinar la logística.		comprendan sus funciones y que todos los miembros de análisis estén dispuestos a participar activamente en el taller. Los documentadores son responsables de registrar la información generada durante los talleres.
1. Construir perfiles de amenaza basados en activos	Procesos 1, 2, 3 y 4	
2. Identificar vulnerabilidades de infraestructura	Procesos 5, 6	
3. Desarrollar estrategias y planes de seguridad	Procesos 7 y 8	

Tabla 1.2-2: Atributos y los resultados del enfoque de OCTAVE

Fuente: Los autores

1.2.2 FASES DEL MÉTODO OCTAVE

1.2.2.1 La Preparación

Durante esta fase sientan las bases para la evaluación, pues sus actividades se refieren a los factores críticos de éxito. En primer lugar, se debe nombrar al "coordinador", que es alguien dentro de la organización que tenga interés en la realización del Método OCTAVE [4 pág. 60]. A continuación se muestra el resumen de los factores críticos de éxito:

Actividad	**Descripción**
Obtener patrocinio de la alta dirección para OCTAVE	El coordinador trabaja con altos directivos de la organización para obtener el patrocinio de la evaluación.
Seleccionar a los miembros del equipo de análisis	El coordinador reúne el equipo de análisis después de obtener el patrocinio de la alta dirección para la evaluación.
Seleccione las áreas operativas para	El equipo de análisis guía a los altos directivos de la organización en la selección de las áreas operativas a

Actividad	Descripción
participar en OCTAVE	examinar durante el Método OCTAVE.
Selección de los participantes	El equipo de análisis selecciona el personal a partir de múltiples niveles de la organización, no debe haber relaciones de subordinación entre los participantes, para así asegurar la comunicación abierta, para participar en los procesos de 1 a 3.
Coordinar la logística	Un miembro del equipo de análisis debe ser el coordinador de logística.

Tabla 1.2-3: Actividades para la preparación del método OCTAVE

Fuente: Los autores

Es necesario que una vez que los miembros del personal y del equipo de análisis se seleccionen, se establezca el cronograma de implementación del método OCTAVE.

Los atributos y los resultados del enfoque de OCTAVE se implementan a través de las fases del método OCTAVE.

1.2.2.2 Fase 1: Construir perfiles de amenaza basados en activos

Esta fase se refiere a la Identificación del conocimiento organizacional, creando un punto de vista organizativo, o global de los problemas de seguridad operacional, determinando qué es importante para la organización y lo que la gente ya está haciendo para proteger lo que ellos creen que es importante, a través de una serie de talleres de educción de conocimiento.

Para llevar a cabo los procesos de esta fase, se requiere el catálogo de prácticas, que son acciones que ayudan a iniciar, implementar y mantener la seguridad dentro de una empresa [5].

Esta fase se basa en activos, un activo es algo de valor a la empresa, e incluye información documentada, sistemas de información (hardware, software e información), hardware, software de aplicación y personas con capacidades difíciles de reemplazar.

Fase 1. Construir perfiles de amenaza basados en activos (visión organizacional)			
Proceso	**Entrada**	**Actividades**	**Participantes**
1. Identificar los conocimientos de la alta directiva.	Catálogo de prácticas	Identificar los activos y las prioridades relativas. Se elegirá los más importantes justificando su elección (no más de 5).	La alta directiva
2. Identificar el conocimiento de la zona de gestión operacional		Identificar las áreas de interés: Por cada activo crítico, que son escenarios que ponen en peligro a los activos más importantes sobre la base de las fuentes típicas de amenaza y sus resultados. Los resultados de una fuente de amenaza, puede ser la revelación, modificación, pérdida o interrupción de la información. Adicionalmente se debe identificar el impacto (o qué pasaría si el escenario efectivamente ocurre). Identificar los requisitos de seguridad (confidencialidad, integridad y disponibilidad) para los activos más importantes y seleccionar el requisito más importante. Capturar el conocimiento de las prácticas actuales de seguridad y vulnerabilidades de la organización.	Mandos medios (zona de gestión operacional)
3. Identificar los conocimientos del personal.			Personal de la organización (TI y negocio por separado)
4. Crear perfiles de amenaza	Activos. Áreas de interés e	La consolidación de información de los procesos de 1 a 3: A través de agrupar por nivel organizacional: los activos,	Equipo de análisis

Fase 1. Construir perfiles de amenaza basados en activos (visión organizacional)			
	impacto.	requisitos de seguridad por activo, y áreas de interés e impacto por activo; permitiendo identificar y consolidar elementos comunes entre niveles. La identificación de las amenazas a los activos críticos: A través del mapeo de las áreas de interés de cada activo crítico al perfil de genérico de riesgo. El mapeo se logra desglosando el área de interés en los componentes del perfil de amenaza que son: activo, acceso, actor, motivo y resultado.	

Tabla 1.2-4: Fase 1 del método OCTAVE, construir perfiles de amenaza basados en activos

Fuente: Los autores

El perfil genérico de amenaza utiliza una forma estructurada de representar amenazas y proporciona resumen completo de todas las amenazas a los activos *[4 pág. 112]*. Su representación se llama árbol de amenaza de activos y emplea las siguientes propiedades: activo, acceso (red o físico), actor (quien puede violar los requisitos de seguridad), motivo (deliberado o accidental), resultado (revelación, modificación, pérdida, interrupción). Por ejemplo, para el activo X (activo), utilizando la red (acceso), una persona (actor humano), de forma accidental (motivo) provoca revelación de la información (resultado).

Por ejemplo, el área de preocupación “personal accediendo a información del sistema X que al que no tiene autorización”, puede traducirse en las propiedades de árbol de amenaza siguientes: sistema X (activo), red (acceso), personal (actor), deliberado (acción), modificación (resultado).

De acuerdo a establecer análisis y mitigación de riesgos, las categorías fuentes de amenaza son diferentes a aquellas que son útiles para obtener áreas de interés, y se muestran a continuación:

Categoría de fuente de amenaza	**Definición**
Los actores humanos con acceso a la red	Basadas en red para los activos críticos de una organización. Requieren la acción directa de una persona y puede ser deliberada o accidental.
Los actores humanos con el acceso físico	Amenazas físicas a los activos críticos de una organización. Requieren la acción directa de una persona y puede ser deliberada o accidental en la naturaleza.
Los problemas del sistema	Defectos de hardware, defectos de software, falta de disponibilidad de sistemas relacionados con el código malicioso, y otros problemas relacionados con el sistema.
Otros problemas	Las amenazas en esta categoría son los problemas o situaciones que escapan al control de una organización. Incluye las amenazas de desastres naturales, la falta de infraestructura crítica.

Tabla 1.2-5: Categorización de amenazas

Fuente: Enfoque OCTAVE

De acuerdo a las 4 categorías de fuentes de amenaza antes mencionadas, se puede crear 4 árboles de amenaza basados en activos, es decir, uno para cada fuente de amenaza (los 4 árboles de amenaza forman el perfil genérico de amenaza). Con una estructura: activo, acceso (si aplica de acuerdo a la categoría de fuente de

amenaza), actor, motivo (si aplica de acuerdo a la categoría de fuente de amenaza) y resultado.

Dado que los activos se relacionan con los requisitos de seguridad, a través de la siguiente relación se puede asociar los requisitos con los tipos de resultado:

Requerimiento de seguridad	**Resultado**
Confidencialidad	Revelación
Integridad	Modificación
Disponibilidad	Pérdida, destrucción, interrupción

Tabla 1.2-6: Requerimientos de seguridad de la información

Fuente: Enfoque OCTAVE

Adicionalmente, hay que tener en cuenta que la categoría de un activo define la categoría de amenaza que se debe considerar, entonces hay que revisar los siguientes criterios en los árboles de amenaza:

Tipo de Activo	**Categoría de amenaza aplicables**
Información electrónica	Los actores humanos con acceso a la red, los actores humanos con el acceso físico, los problemas de los sistemas, y otros problemas
Información física	Los actores humanos con el acceso físico y otros problemas
Sistemas en general, software y hardware	Los actores humanos con acceso a la red, los actores humanos con el acceso físico, los problemas de los sistemas, y otros problemas
Software (servicios)	Los actores humanos con acceso a la red, los actores humanos con el acceso físico, los problemas de los sistemas, y otros problemas
Hardware	Los actores humanos con el acceso físico y otros problemas.
Personas	Otros problemas

Tabla 1.2-7: Categorías de amenaza por tipos de activo

Fuente: Los autores

A modo de ejemplo a continuación se muestra un árbol de amenaza para un activo, concluido el proceso 4, para esto, se basó en el perfil genérico respectivo:

Activo	Acceso	Actor	Motivo	Resultado	Áreas de interés
				Revelación	1
			Accidental	Modificación	
				Pérdida	
		Interno		Interrupción	
				Revelación	
			Deliberado	Modificación	2, 3
				Pérdida	3
Sistema X	Red			Interrupción	
				Revelación	
			Accidental	Modificación	
				Pérdida	
		Externo		Interrupción	3
				Revelación	
			Deliberado	Modificación	
				Pérdida	
				Interrupción	

Tabla 1.2-8: Ejemplo de árbol de amenaza

Fuente: Los autores

En la gráfica anterior la línea punteada quiere decir que no hay riesgo.

1.2.2.3 Fase 2: Identificar las vulnerabilidades de la infraestructura

El objetivo principal de esta fase es la identificación de debilidades tecnológicas en la infraestructura informática. Las vulnerabilidades de tecnología son las debilidades en los sistemas, dispositivos y componentes que pueden conducir directamente a la acción no autorizada [6]. A continuación se muestra las categorías más comunes:

Categoría de vulnerabilidad	**Descripción**
De diseño	Inherente en el diseño o las especificaciones de hardware o software.
De la implementación	Error cometido en la aplicación de software o hardware de un diseño satisfactorio.
De la configuración	Error en la configuración y administración de un sistema o

	componente.

Tabla 1.2-9: Categorización de vulnerabilidades

Fuente: Los autores

Las vulnerabilidades de diseño e implementación pueden llegar a transformarse en vulnerabilidades de configuración. Por tanto en una evaluación de los riesgos de seguridad de información operativa, hay que centrarse principalmente en las vulnerabilidades de configuración [4 pág. 140].

A continuación se muestra las áreas de práctica operacional en el catálogo de prácticas:

Áreas de práctica operacional

Seguridad física	**Seguridad de tecnología de información**	**Seguridad de personal**
Planes y procedimientos de seguridad física	Administración de sistemas y redes	Gestión de incidentes
Control de acceso físico	Monitoreo y auditoría de seguridad de TI	Prácticas generales del personal
Monitoreo y auditoría de seguridad física	Autenticación y autorización	
	Cifrado	
	Gestión de vulnerabilidad	
	Herramientas de administración de sistemas	
	Diseño y arquitectura de seguridad	

Tabla 1.2-10: Áreas de práctica operacional

Fuente: Enfoque OCTAVE

A continuación se detalla las actividades por cada proceso de esta fase:

Fase 2. Identificar las vulnerabilidades de la infraestructura (visión tecnológica)			
Proceso	**Entrada**	**Actividades**	**Participantes**
5. Identificar los componentes clave	Topología de red (con todos los accesos) , herramientas de mapeo, listados de priorización de computadores	Seleccionar los componentes de la infraestructura a evaluar, a través de Identificar las clases de los componentes clave asociados a las rutas de acceso a los perfiles de amenaza, enfocándose en los que están relacionados a actores humanos usando acceso a red o físico.	Equipo de análisis y los miembros seleccionados del personal de TI.
6. Evaluación de Componentes seleccionados	Catálogo de vulnerabilidades	Ejecución de las herramientas de evaluación de la vulnerabilidad: En los componentes de infraestructura seleccionados en el proceso 5 en base al catálogo de vulnerabilidades. Revisión de las vulnerabilidades. Refinar el resumen: Generando las acciones y recomendaciones. Realizar un análisis de brechas.	

Tabla 1.2-11: Fase 2 del método OCTAVE, Identificar las vulnerabilidades de la infraestructura

Fuente: Los autores

A continuación se muestra la relación entre las categorías de activos y los sistemas de interés:

Categoría de Activo	Sistema de interés
Activos de sistemas	Es el activo
Activos de información	Es el sistema más relacionado con la información
Activos de software	Es el sistema más relacionado con la aplicación o servicio.

Tabla 1.2-12: Categorización de activos vs Sistemas de interés

Fuente: Los autores

Un activo crítico puede estar relacionado a varios sistemas de interés, en caso de que el activo crítico se define de manera demasiado amplia, se podría definir de manera más estrecha o dividirla en pequeños activos críticos. Alternativamente, se puede aceptar que se tenga varios sistemas de interés.

Las clases de componentes principales de un sistema de interés son: servidores, componentes de red, componentes de seguridad, estaciones de trabajo, laptops, dispositivos de almacenamiento, dispositivos inalámbricos, y otros. Estas clases de componentes deben ser obtenidas analizando el acceso a los activos a través de estos componentes ya sea de forma legítima como no autorizada.

Para la evaluación, es necesario definir quien la llevará a cabo (internamente o expertos externos), las herramientas a utilizar, quien interpretará los resultados.

A continuación se muestra el cuadro referencial de ejemplo de componentes claves evaluar:

Componente clave	**Dirección IP**	**Enfoque**	**Herramientas**	**Justificación**
Equipo X (de la clase servidores)	……	Experto externo, Staff interno, Proveedor de servicios	Escáner de funcionamiento, de redes, híbridos, listas de verificación, scripts. (gratuitos, con costo)	…

Tabla 1.2-13Ejemplo de clases de componentes claves a evaluar

Fuente: Los autores

Las herramientas de vulnerabilidad tienen limitaciones. No indican cuándo algunos de los procedimientos de administración del sistema están siendo utilizados indebidamente o se realizan incorrectamente [4 pág. 156].

La ejecución de la evaluación de vulnerabilidad con las respectivas herramientas arrojará información como nombre, descripción, nivel de gravedad y medidas a aplicar relacionadas con la vulnerabilidad detectada.

1.2.2.4 Fase 3: Desarrollar la estrategia y planes de seguridad

En esta fase se examinará cómo las amenazas a los activos críticos de la organización pueden afectar a los objetivos de negocio y su misión, posteriormente se desarrollará soluciones estratégicas y tácticas diseñadas para manejar la incertidumbre que su organización enfrenta debido a los riesgos de seguridad de información

Fase 3. Desarrollar la estrategia y planes de seguridad (análisis de riesgo)			
Proceso	**Entrada**	**Actividades**	**Participantes**
7. Conduciendo el Análisis de Riesgo	Áreas de interés. Perfil de amenaza	Identificar y analizar los riesgos. Identificar el impacto de las amenazas por resultado en relación a la misión organizacional, a través de descripciones narrativas de las repercusiones a la organización.	Equipo de análisis y personal suplementario.
	Planes organizacionales, requisitos legales, resultados de otros procesos de gestión de riesgos.	Creación de criterios de evaluación de riesgos: Definiendo lo que constituye un impacto alto, medio y bajo para cada área de impacto (reputación, seguridad, productividad, multas, financiero, etc.).	
	Perfil de amenaza. Descripción de	La evaluación del impacto de las amenazas: a los activos críticos, revisando las descripciones de	

Fase 3. Desarrollar la estrategia y planes de seguridad (análisis de riesgo)			
	impacto. Criterio de evaluación de riesgo.	impacto por activo crítico por tipo de resultado, a continuación debe asociar una medida de impacto a la descripción utilizando los criterios de evaluación.	
	Planes organizacionales, requisitos legales, resultados de otros procesos de gestión de riesgos.	Si se incorpora probabilidad : Describir la probabilidad de amenazas a los activos críticos. Crear criterios de probabilidad de la evaluación: Medidas contra las cuales se evaluará cada amenaza. Evaluar la probabilidad de las amenazas a los activos críticos	
8. Fomentar la Estrategia de Protección	Catálogo de prácticas Prácticas actuales de seguridad. Áreas de preocupación Perfiles de riesgo. Acciones recomendadas en base a vulnerabilidad (proceso 6).	Priorizar la mitigación de riesgo, se usa el valor o pérdida esperada. Consolidar la información de los procesos de 1-3. Asociar cada práctica de seguridad con las vulnerabilidades de la organización de acuerdo a las áreas de práctica. Revisar la información de riesgos. Crear una estrategia de protección que incluye las estrategias de seguridad para las áreas de práctica, de orientación	Taller 1: Equipo de análisis y miembros seleccionados de la organización (miembro de planificación estratégica).

Fase 3. Desarrollar la estrategia y planes de seguridad (análisis de riesgo)			
		a futuro tendiente a largo plazo. Posteriormente, se debe definir las estrategias de seguridad para las áreas de práctica operacional. Crear planes de mitigación: Son acciones operativas asociadas a las actividades necesarias para mitigar los riesgos y amenazas a los activos críticos. Seleccionar el enfoque de mitigación por cada riesgo. Revisar los planes de mitigación para buscar coherencia entre sí, de haber alguna brecha, incorporarla en la estrategia. El perfil de riesgo debe ser completado con el enfoque y el plan de mitigación. Crear lista de acciones: La organización puede tomarlas en el corto plazo sin la necesidad de formación especializada.	
		Se presenta la estrategia de protección propuesta, los planes de mitigación, y la lista de acciones a los altos directivos de la organización.	Taller 2: Equipo de análisis y altos directivos de la organización.

Tabla 1.2-14: Fase 3 del método OCTAVE, Desarrollar la estrategia y planes de seguridad

Fuente: Los autores

El riesgo es la posibilidad de sufrir un daño o pérdida. Es el potencial para la realización de consecuencias negativas no deseadas de un evento. Un riesgo se compone de un evento, la incertidumbre, y una consecuencia. El evento se relaciona con la amenaza y para muchas metodologías de riesgo, la incertidumbre se representa con la probabilidad de ocurrencia, por último la consecuencia es el impacto resultante en la organización debido a una amenaza. La probabilidad es muy subjetiva, en ausencia de datos objetivos y debe usarse con cuidado en el análisis de riesgos, dado que no se cuenta con datos objetivos acerca de los actores humanos que explotan vulnerabilidades conocidas, es difícil utilizar un método de pronóstico basado en probabilidades. Debido a esto, OCTAVE se centra en una técnica de análisis basada en la planificación de escenarios.

Para realizar el taller del proceso 7, es necesario refrescar las áreas de interés y perfiles de amenaza.

A continuación se muestra un ejemplo de referencia de descripción de impacto por activo:

Activo	**Resultado**	**Descripción de Impacto**
Activo X	Modificación	Puede afectar la productividad

Tabla 1.2-15: Ejemplo de descripción de impacto por activo

Fuente: Los autores

A continuación se muestra un ejemplo referencial de criterio de evaluación:

Área de impacto	**Alto**	**Medio**	**Bajo**
Reputación	Más de 30% de pérdida de confianza de cliente.	Del 10% al 30% de pérdida de confianza de cliente.	Menos del 10% de pérdida de confianza de cliente.

Tabla 1.2-16: Ejemplo de criterio de evaluación por área de impacto

Fuente: Los autores

Se define la probabilidad como la posibilidad de que un evento ocurra. OCTAVE incorpora el criterio de probabilidad en el análisis de riesgos por su gran popularidad.

En seguridad de la información, la estimación de la probabilidad se basa en utilizar la frecuencia de ocurrencia, sin embargo es difícil que se cuente con datos históricos.

A continuación se muestra un ejemplo referencial de criterio de probabilidad:

Frecuencia de ocurrencia	**Alta**	**Media**	**Baja**
	Mayor a 12 veces al año	De una a 11 veces al año	Menos a una vez al año

Tabla 1.2-17: Ejemplo de criterio de probabilidad

Un perfil de amenaza, incorporado impacto y probabilidad, genera un perfil de riesgo:

Activo	Acceso	Actor	Motivo	Resultado	Áreas de interés	Impacto	Probabilidad
				Revelación	1	Medio	Alta
			Accidental	Modificación		Alto a medio	Alta
				Pérdida		Alto	Alta
		Interno		Interrupción		Alto	Baja
				Revelación		Medio	Media
			Deliberado	Modificación	2, 3	Alto a medio	Baja
				Pérdida	3	Alto	Baja
Sistema X	Red			Interrupción		Alto	Baja
				Revelación			
			Accidental	Modificación			
				Pérdida			
		Externo		Interrupción			
				Revelación		Medio	Baja
			Deliberado	Modificación	3	Alto a Medio	Baja
				Pérdida		Alto	Baja
				Interrupción		Alto	Media

Tabla 1.2-18: Ejemplo de perfil de riesgo con probabilidad e impacto

Fuente: Los autores

La consolidación de datos de los procesos 1-3, acerca de las prácticas de seguridad, se consolidan de acuerdo al siguiente ejemplo referencial:

Área de práctica: Conciencia y entrenamiento en seguridad				
Enunciado de encuesta	**Alta Directiva**	**Mandos medios**	**Personal**	**Personal de TI**
El personal entiende sus roles y responsabilidades en seguridad, está documentado y verificado	Si No No está claro	Si No No está claro	Si No No está claro	Si No No está claro
Nivel organizacional	**Práctica de seguridad**		**Vulnerabilidad**	
Alta directiva/Mandos medios/Persona/Personal de TI	Se tiene entrenamiento, guía, regulaciones, políticas.		El personal entiende los sistemas pero no gestiona incidentes ni reconoce anomalías.	

Tabla 1.2-19: Ejemplo de consolidación de información de procesos 1-3

Fuente: Los autores

El establecimiento de la estrategia de protección, se genera alrededor de las áreas estratégicas del catálogo de prácticas. Adicionalmente se analiza las áreas de práctica principal de operaciones. La estructura de la estrategia de protección, tendría la siguiente forma referencial:

Área (Estratégica/Operacional)	**Estrategia de protección**
Seguridad de TI	Desarrollar un plan de modernización de servicios de seguridad

Tabla 1.2-20: Ejemplo de estrategia de protección

Fuente: Los autores

En este punto, el perfil de riesgo, quedaría con la estructura siguiente:

Un perfil de riesgo culminado el proceso 8A, se vería de la siguiente forma:

Activo	Acceso	Actor	Motivo	Resultado	Impacto	Enfoque	Plan de mitigación
				Revelación	Medio	Mitigar	Lista de los planes, todos aplicarían para todas las ramas de este perfil de riesgo
			Accidental	Modificación	Alto a medio	Mitigar	Se puede añadir medidas específicas de apoyo al éxito del plan.
				Pérdida	Alto	Mitigar	
		Interno		Interrupción	Alto	Mitigar	
				Revelación	Medio	Mitigar	
			Deliberado	Modificación	Alto a medio	Mitigar	
				Pérdida	Alto	Mitigar	
Sistema X	Red			Interrupción	Alto	Mitigar	
				Revelación			
			Accidental	Modificación			
				Pérdida			
		Externo		Interrupción			
				Revelación	Medio	Mitigar	
			Deliberado	Modificación	Alto a Medio	Mitigar	
				Pérdida	Alto	Mitigar	
				Interrupción	Alto	Mitigar	

Tabla 1.2-21: Ejemplo de perfil de riesgo con enfoque y plan de mitigación

Fuente: Los autores

En contexto de la toma de decisiones de mitigación de riesgos, el valor esperado (exposición al riesgo) para un riesgo es el producto de la pérdida potencial que podría ocurrir (o el valor del impacto) multiplicada por su frecuencia de ocurrencia proyectada (o probabilidad) [4 pág. 221]; esto en un análisis cuantitativo. Sin embargo, de acuerdo a un análisis cualitativo, sirve de ayuda la matriz de valor esperado siguiente:

		Probabilidad		
		Alta	**Media**	**Baja**
Impacto	**Alto**	Alto	Alto	Medio
	Medio	Alto	Medio	Bajo
	Bajo	Medio	Bajo	Bajo

Tabla 1.2-22: Matriz de valor

Fuente: Enfoque OCTAVE

Muy comúnmente, el valor esperado se utiliza para establecer prioridades, esto conlleva al problema de tratar con igual prioridad a eventos catastróficos con muy baja prioridad y alto impacto con eventos de alta probabilidad pero de bajo impacto.

A continuación se muestra un perfil de riesgo considerando el valor esperado:

Activo	Acceso	Actor	Motivo	Resultado	Impacto	Probabilidad	Valor esperado
				Revelación	A	A	A
			Accidental	Modificación	A-M	A	A
				Pérdida	A	A	A
		Interno		Interrupción	A	B	M
				Revelación	M	M	M
			Deliberado	Modificación	A-M	B	M-B
				Pérdida	A	B	M
Sistema X	Red			Interrupción	A	B	M
				Revelación			
			Accidental	Modificación			
				Pérdida			
		Externo		Interrupción			
				Revelación	A	B	B
			Deliberado	Modificación	A-M	B	M-B
				Pérdida	A	B	M
				Interrupción	A	M	A

Tabla 1.2-23: Ejemplo de perfil de riesgo considerando el valor esperado

Fuente: Los autores

1.2.3 LA NATURALEZA NO LINEAL DEL MÉTODO OCTAVE

Pareciera que en el Método OCTAVE al completar un proceso, ya puede pasar al siguiente. Sin embargo, como seguridad de la información trata temas tan complejos organizativos y tecnológicos, no se presta a un proceso lineal ni repetitivo. Hay muchos posibles bucles de retroalimentación en el método.

1.2.4 VARIACIONES EN EL MÉTODO OCTAVE

Una adaptación es casi cualquier opción que no viola el conjunto básico de requisitos del método OCTAVE, la forma en que las organizaciones optan por aplicar el enfoque OCTAVE variará en función de las características de cada organización.

CAPÍTULO 2
DEFINICIÓN DEL ESQUEMA DE ACOPLAMIENTO DE LA NORMA ISO/IEC 27005:2008 CON EL MÉTODO OCTAVE

2.1 ESQUEMA METODOLÓGICO PARA EL ACOPLAMIENTO

Con el objetivo de dar soporte a la gestión de riesgos de seguridad de la información, se busca el acoplamiento de los lineamientos para gestión de riesgos de seguridad de la información provistos por parte de la norma ISO/IEC 27005:2008 y con las actividades sistemáticas para evaluación y planificación estratégica de riesgos de seguridad de la información propuestos por el método OCTAVE.

La norma ISO/IEC 27005:2008 propone un enfoque de un proceso de gestión de riesgos de seguridad de la información basado en actividades. El método OCTAVE consiste en tres fases con ocho procesos basados en actividades. De acuerdo a esto, para determinar el acoplamiento, se ha encontrado que el nivel de granularidad más bajo que se maneja en ambos modelos está enfocado a la ejecución de actividades, por tanto, el enfoque de análisis de acoplamiento estará asociado a las actividades.

A continuación se presenta un esquema comparativo básico inicial entre la norma ISO/IEC 27005:2008 y el método OCTAVE de acuerdo a los componentes de la gestión de riesgos (evaluación y el tratamiento):

Componentes de gestión de riesgos	**ISO/IEC 27005:2008**	**Método OCTAVE**
Evaluación	Establecimiento del contexto. Valoración del riesgo: - Análisis del riesgo:	Construir perfiles de amenaza basados en activos. Identificar vulnerabilidades de infraestructura.

	(Identificación y estimación del riesgo). - Evaluación del riesgo.	
Tratamiento	Tratamiento del riesgo Aceptación del riesgo.	Desarrollar planes y estrategias de seguridad
Componentes adicionales	Monitoreo y revisión del riesgo Comunicación del riesgo	Criterios de OCTAVE: Principios y atributos del enfoque OCTAVE.

Tabla 2.1-1: Comparativa inicial de la norma ISO/IEC 27005:2008 y el método OCTAVE

Fuente: Los autores

Del cuadro anterior, se puede observar que ambos modelos cubren la evaluación y tratamiento del riesgo, sin embargo la norma ISO/IEC 27005:2008 abarca adicionalmente el monitoreo y comunicación del riesgo. Por tanto, y de acuerdo a determinar el esquema de acoplamiento entre ambos modelos, se propone partir de la norma ISO/IEC 27005:2008 como referencia principal, por abarcar en sus actividades más allá de la evaluación y tratamiento, adicionalmente debido también a que la norma ISO/IEC 27005:2008 es más actual que el método OCTAVE.

En el proceso de determinación del esquema de acoplamiento, inicialmente se realizará un análisis comparativo buscando aquellas actividades en común de ambos modelos, también se detectará aquellas actividades sin correspondencia; posteriormente, sobre el conjunto de actividades comparadas se determinará las oportunidades acoplamiento, tomando en cuenta que la referencia es la norma ISO/IEC 27005:2008. Finalmente en base de las oportunidades de acoplamiento se determinará el esquema de acoplamiento resultante, sobre las actividades elegidas para el efecto. Es decir serán todas las actividades propuestas por la norma ISO/IEC 27005:2008 las que forme parte del esquema de acoplamiento, que incluyen las actividades en común con el método OCTAVE; sin embargo, se adicionarán actividades específicas del método OCTAVE de acuerdo a fortalecer el esquema y no se tomarán en cuenta otras.

De acuerdo a lo descrito anteriormente, el esquema de acoplamiento esperado se describe en la siguiente gráfica:

Figura 2.1-1 Esquema de acoplamiento

Fuente: Los autores

2.2 ANÁLISIS COMPARATIVO DE LA NORMA ISO/IEC 27005:2008 CON EL MÉTODO OCTAVE

A continuación se realizará un análisis comparativo de las actividades de la norma ISO/IEC 27005:2008 en relación con las del Método OCTAVE, en busca de actividades comunes. La comparación se realizará de forma secuencial y de acuerdo al orden propuesto en cada modelo. Conforme se avance con la comparación se procederá a ordenar las actividades ya sea que estas tengan o no una actividad similar, de tal forma que el conjunto de todas las actividades comparadas tenga una secuencia lógica, considerando la precedencia que tiene la norma ISO/IEC 27005:2008 como referencia del esquema de acoplamiento. Finalmente se obtendrá el conjunto de todas las actividades de ambos modelos, ordenados secuencialmente, con una descripción comparativa.

Con el objetivo de comprender el esquema comparativo, en el Anexo 1 se muestra la nomenclatura para la norma ISO/IEC 27005:2008 y el método OCTAVE.

A continuación se muestra el análisis comparativo por fases, procesos y actividades en orden lógico para el método OCTAVE y la norma ISO/IEC 27005:2008. Se ha

utilizado el acrónimo MO para referirse al método OCTAVE y el acrónimo NI para referirse a la norma ISO/IEC 27005:2008.

Norma ISO/IEC 27005:2008 ---------- Método OCTAVE	**Descripción comparativa**
A1 Preparación	**Descripción de actividades:** MO: Se definirá al "coordinador" que será de quien surja la iniciativa de implementar acciones asociadas a la gestión de riesgos de seguridad de la información. **Fuentes:** MO: No aplica. **Participantes:** MO: El coordinador. **Resultados:** MO: Definición del coordinador.
A2 Obtener patrocinio de la alta dirección para OCTAVE	**Descripción de actividades:** MO: El coordinador trabaja con los altos directivos de la organización para obtener el patrocinio de la evaluación. MO: Concientizar a los altos directivos de que deben considerar de que la seguridad informática no es solamente un problema de tecnología de la información. **Fuentes:** MO: No aplica. **Participantes:** MO: El coordinador **Resultados:** MO: Patrocinio de la alta dirección.
	Descripción de actividades:

Norma ISO/IEC 27005:2008 ---------- Método OCTAVE	**Descripción comparativa**
A3 Seleccionar a los miembros del equipo de análisis	MO: El coordinador reúne el equipo de análisis después de obtener el patrocinio de la alta dirección para la evaluación. MO: Familiarizar al equipo de análisis con el método OCTAVE. MO: Componer el núcleo del equipo de análisis de tres a cinco personas de las unidades de negocio de la organización y el departamento de tecnología de la información, la mayoría son de las unidades de negocio de la organización. MO: Integrar al menos un miembro que tenga familiaridad con la tecnología de la información y las cuestiones de seguridad. **Fuentes:** MO: No aplica. **Participantes:** MO: El coordinador. **Resultados:** MO: Equipo de análisis conformado
A4 Definir el alcance **A5** Definir los límites	**Descripción de actividades:** MO: El equipo de análisis guía a los altos directivos de la organización en la selección de las áreas operativas a examinar durante el Método OCTAVE.
A4 Seleccione las áreas operativas para participar en OCTAVE	MO: Se recomienda al menos cuatro zonas operativas; se recomienda en general, una de las cuales debe ser la tecnología de la información. NI: El alcance se define para asegurar que los activos relevantes son tomados en cuenta en la valoración de riesgos, cada exclusión del alcance se justifica. NI: Los límites localizan aquellos riesgos que quizá salen del

Norma ISO/IEC 27005:2008 ---------- Método OCTAVE	**Descripción comparativa**
	contexto. **Fuentes:** MO: No aplica. **Participantes:** MO: El equipo de análisis **Resultados:** MO: Áreas operativas a participar NI: Límites y alcance
A5 Selección de los participantes	**Descripción de actividades:** MO: El equipo de análisis selecciona el personal a partir de múltiples niveles de la organización, no debe haber relaciones de subordinación entre los participantes, para así asegurar la comunicación abierta, para participar en los procesos de 1 a 3. Hay que asegurarse de que ninguna información discutida en un taller se atribuye a un individuo específico. MO: Si es necesario, aumentar las capacidades para los procesos de 4 a 8 lo hace mediante la inclusión de participantes adicionales. **Fuentes:** MO: No aplica. **Participantes:** MO: El equipo de análisis. **Resultados:** MO: Participantes seleccionados.
A6	**Descripción de actividades:** MO: Un miembro del equipo de análisis debe ser el coordinador

Norma ISO/IEC 27005:2008 ---------- Método OCTAVE	**Descripción comparativa**
Coordinar la logística	de logística, debe asegurarse de que todo está disponible, e informar a todos los participantes cuándo y dónde se realizarán talleres. **Fuentes:** MO: No aplica. **Participantes:** MO: El equipo de análisis. **Resultados:** MO: No aplica.
A12 Determinar una metodología de estimación de riesgo	**Descripción de actividades:** NI: La metodología de estimación del riesgo, indica como valorar el impacto y la probabilidad, que puede ser cualitativa, cuantitativa o una combinación; debe ser consistente con el criterio de evaluación del riesgo. **Fuentes:** NI: Datos históricos, criterio de evaluación de riesgo. **Participantes:** NI: No aplica. **Resultados:** NI: Metodología de estimación del riesgo.
A1 Definir el criterio básico de evaluación de riesgo.	**Descripción de actividades:** NI: Permitirá evaluar y priorizar los riesgos, en base al valor estratégico de los procesos del negocio, la criticidad de los activos de información, requerimientos legales y contractuales, expectativas y percepciones de los interesados y consecuencias negativas en la reputación.

<table>
<tr><th>Norma ISO/IEC 27005:2008

Método OCTAVE</th><th>Descripción comparativa</th></tr>
<tr><td></td><td>Fuentes:
NI: Información relevante de la organización.
Participantes:
NI: No aplica.
Resultados:
NI: Criterio básico de evaluación de riesgo.</td></tr>
<tr><td>A2
Definir el criterio básico de impacto</td><td rowspan="2">Descripción de actividades:
MO: Definir lo que constituye un impacto alto, medio y bajo para cada área de impacto (reputación, seguridad, productividad, multas, financiero, etc.), en base a la comprensión de los límites de riesgo ya existentes de la organización sobre la base de planes estratégicos y operativos, la responsabilidad, y las cuestiones relacionadas con el aseguramiento.
NI: El criterio de impacto permitirá valorar las consecuencias (impacto al negocio que provocan pérdida de confidencialidad, integridad y disponibilidad de la información), se especifica de acuerdo al daño o costo para la organización a causa de un evento de seguridad de la información, considerando el tipo de activo impactado, la brecha de seguridad, deterioro de operaciones, pérdida de valor de negocio o financiero, ruptura de planes o plazos, daño a la reputación y brechas de regulaciones legales y contractuales.
NI: El criterio de impacto Indicará cuando el impacto es Alto, Medio o Bajo.
Fuentes:
MO: Planes organizacionales, requisitos legales, resultados de</td></tr>
<tr><td>A29
Creación de criterios de evaluación de riesgos</td></tr>
</table>

Norma ISO/IEC 27005:2008 ---------- Método OCTAVE	**Descripción comparativa**
	otros procesos de gestión de riesgos. NI: Información relevante de la organización. NI: Datos históricos, criterio de evaluación de riesgo. **Participantes:** MO: Equipo de análisis, personal suplementario. **Resultados:** MO: Criterio de evaluación de riesgo. NI: Criterio básico de impacto.
A3 Definir el criterio básico de aceptación de riesgo	**Descripción de actividades:** NI: Definir el criterio de aceptación del riesgo, cada organización define su propia escala, se especifica en base a las políticas, metas, objetivos organizacionales e intereses de los interesados.
	Fuentes: NI: Información relevante de la organización. **Participantes:** NI: No aplica. **Resultados:** NI: Criterio básico de aceptación de riesgo

Tabla 2.2-1 Descripciones comparativas detalladas de la norma ISO/IEC 27005:2008 y el método OCTAVE

Fuente: Los autores

Las descripciones comparativas detalladas, completas, para todas las actividades pueden encontrarse en el Anexo 2.

2.3 ANÁLISIS DE OPORTUNIDADES DE ACOPLAMIENTO DE COMPONENTES DE LA NORMA ISO/IEC 27005:2008 CON EL MÉTODO OCTAVE

De acuerdo a la descripción comparativa detallada en la tabla anterior, se puede observar las siguientes similitudes y diferencias generales entre el método OCTAVE y la norma ISO/IEC 27005:2008, con el objetivo de determinar las oportunidades acoplamiento.

Similitudes:

- El enfoque está asociado tanto al negocio como a TI.
- Basan su evaluación de riesgos de seguridad de la información alrededor de activos.
- Utilizan un enfoque de fases asociado a la gestión de riesgos de seguridad de la información.
- Ambos consideran técnicas orientadas a la utilización de escenarios.

Diferencias:

- El método OCTAVE propone un enfoque basado en principios y atributos que aplican a todas las fases propuestas, la norma ISO/IEC 27005:2008 propone únicamente el proceso.
- EL método OCTAVE proporciona detalle del como ejecutar las fases, detallando actividades, participantes, entradas, resultados y formularios. La norma ISO/IEC 27005:2008 únicamente propone que se debe realizar en cada fase.

A continuación, se determinará las oportunidades de acoplamiento en base a las descripciones comparativas de la sección anterior, indicando si se mantiene, no se mantiene o se consolida las actividades comparadas. Se debe tomar en cuenta que la referencia para el acoplamiento es la norma ISO/IEC 27005:2008, por lo que todas

sus actividades serán mantenidas, mientras que las del método OCTAVE podrían ser o no mantenidas en el esquema de acoplamiento.

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
A1 Preparación	**Descripción de acoplamiento:** Mantener esta actividad como previa a todo el proceso de implementación del modelo de gestión de riesgos de seguridad de la información. **Nombre de actividad acoplada:** Preparación. **Ventaja:** Definir formalmente al coordinador de la implementación del modelo de gestión de riesgos de seguridad de la información permite apalancar el surgimiento de la iniciativa de implementación. **Desventaja:** Ninguna. **Consideraciones:** La norma ISO/IEC 27005:2008 no hace referencia explícita a esta actividad.
A2 Obtener patrocinio de la alta dirección para OCTAVE	**Descripción de acoplamiento:** Mantener esta actividad como posterior a las actividades intrínsecas de preparación para el proceso, en la cual una vez que se cuente con el coordinador, éste gestionará la obtención del patrocinio de la alta dirección para la implementación del modelo de gestión de riesgos de seguridad de la información. **Nombre de actividad acoplada:** Obtener patrocinio de la alta dirección. **Ventaja:**

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
	El patrocinio de la alta dirección permite apalancar el comprometimiento de los participantes y de los recursos necesarios para llevar a cabo los procesos de gestión de riesgos de seguridad de la información. **Desventaja:** Ninguna. **Consideraciones:** Para el modelo de gestión de riesgos de seguridad de la información propuesto, el coordinador gestionará el patrocinio de la alta dirección para la implementación de dicho modelo. La norma ISO/IEC 27005:2008 no hace referencia explícita a esta actividad. El obtener el patrocinio de la alta dirección, es una actividad del método OCTAVE que se ha asociado a la implementación del modelo de gestión de riesgos de seguridad de la información, en lugar de a una evaluación de riesgos.
A3 Seleccionar a los miembros del equipo de análisis	**Descripción de acoplamiento:** Mantener esta actividad en el proceso, como lo propone el método OCTAVE. **Nombre de actividad acoplada:** Seleccionar a los miembros del equipo de análisis. **Ventaja:** Contar formalmente con la designación del equipo que ejecuta los procesos de evaluación y definición del tratamiento al riesgo; apalancará el análisis de información durante la implementación del modelo. **Desventaja:**

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
	Ninguna. **Consideraciones:** La norma ISO/IEC 27005:2008 no define quien participa en cada actividad del proceso de gestión de riesgos de seguridad de la información. Seleccionar los miembros del equipo de análisis, es una actividad del método OCTAVE que se ha asociado a la implementación del modelo de gestión de riesgos de seguridad de la información, en lugar de a una evaluación de riesgos. Se recomienda que el núcleo de equipo de análisis se conforme con miembros del área de seguridad de la información de la organización, debido a que esto proporcionaría independencia respecto al área de tecnología. El método OCTAVE no hace esta recomendación.
A4 Definir el alcance **A5** Definir los límites **A4** Seleccione las áreas operativas para participar en OCTAVE	**Descripción de acoplamiento:** Consolidar esta actividad definiendo formalmente el alcance de los procesos de gestión de riesgos, a través de establecer qué áreas operativas asociadas a procesos de negocio van a participar. **Nombre de actividad acoplada:** Definir el alcance. **Ventaja:** Contar con el alcance de acuerdo a los activos asociados a las áreas o procesos del negocio elegidos para el efecto, permite claramente conocer que va a ser evaluado y que no. **Desventaja:** Ninguna.

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
	Consideraciones: El alcance debe definirse previamente a empezar los procesos de gestión de riesgo de seguridad de la información. Definir los límites y alcance son actividades de la norma ISO/IEC 27005:2008 que son similares a la selección de áreas operativas en el método OCTAVE, este recomienda cuatro zonas operativas, sin embargo, se ha dejado abierta esta posibilidad en vista de elegir la cantidad adecuada de acuerdo a la naturaleza y necesidades especificas de la organización, lo que podría llevar a que una implementación del modelo de gestión de riesgos de seguridad de la información, por ejemplo, no se refiera a un proceso completo de la cadena de valor, sino a una parte de este.
A5 Selección de los participantes	**Descripción de acoplamiento:** Mantener esta actividad, definiendo formalmente los participantes para los talleres del proceso de gestión de riesgos de seguridad de la información. **Nombre de actividad acoplada:** Selección de los participantes. **Ventaja:** Conocer claramente quien va a participar en los procesos, permite mejorar la gestión de los recursos. **Desventaja:** Ninguna. **Consideraciones:** La norma ISO/IEC 27005:2008 no define quien participa en cada actividad del proceso de gestión de riesgos, sin embargo, el

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
	método OCTAVE lo hace; para el modelo de gestión de riesgos de seguridad de la información propuesto, la selección de participantes aplicará a las actividades definidas por este para el efecto. Seleccionar los participantes es una actividad del método OCTAVE, que se relaciona con los talleres, la elección de participantes es dinámica de acuerdo a las necesidades específicas de cada taller, aun cuando hay una definición inicial, podría requerirse de cambios o personal adicional con conocimientos específicos. El método OCTAVE propone elegir a los participantes a partir de múltiples niveles de la organización (alta directiva, los mandos medios y el personal), para evitar relaciones de subordinación entre los participantes, para así asegurar la comunicación abierta. Sin embargo esto implica mayor cantidad de talleres y actividades adicionales de consolidación de información que incrementan los tiempos de implementación, por lo que se ha optado por elegir a los participantes de acuerdo a su conocimiento y experiencia en los procesos, independientemente de la relación a nivel de organización que estos tengan.
A6 Coordinar la logística	**Descripción de acoplamiento:** No mantener esta actividad, pues puede considerarse como intrínseca a las actividades de previas a la evaluación, es decir debido a su complejidad e importancia, no amerita que conste formalmente como actividad. **Nombre de actividad acoplada:**

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
	No aplica. **Ventaja:** Considerar la coordinación de la logística como intrínseca a las actividades de preparación para la evaluación pues permite consolidar un modelo más compacto con menos actividades. **Desventaja:** Ninguna. **Consideraciones:** La norma ISO/IEC 27005:2008 no propone quien coordinará la logística en proceso de gestión de riesgos.
A12 Determinar una metodología de estimación de riesgo	**Descripción de acoplamiento:** Mantener esta actividad, pues determina en base a la evaluación del impacto y la probabilidad (cuantitativa/cualitativa), como se va a estimar el riesgo. **Nombre de actividad acoplada:** Determinar la metodología de estimación de riesgo. **Ventaja:** Contar con una metodología de estimación de riesgo permite agilitar la evaluación del impacto, probabilidad y riesgo; pues proporciona estos lineamientos. **Desventaja:** Ninguna. **Consideraciones:** El método OCTAVE implícitamente establece que hay que definir un enfoque cuantitativo/cualitativo para la valoración de impacto y probabilidad, la norma ISO/IEC 27005:2008 lo hace explícitamente como una actividad.

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
A1 Definir el criterio básico de evaluación de riesgo.	**Descripción de acoplamiento:** Mantener esta actividad como previa a la evaluación de riesgos, como lo propone la norma ISO/IEC 27005:2008. **Nombre de actividad acoplada:** Definir el criterio básico de evaluación de riesgo. **Ventaja:** Proporcionar desde el inicio del proceso el conocimiento de cómo evaluar el riesgo de acuerdo a priorizar el tratamiento posterior, permitirá enfocar la determinación del resto de criterios básicos acorde a un enfoque común. **Desventaja:** Al ubicar esta actividad antes de las actividades de evaluación de riesgo, de acuerdo a lo que indica la norma ISO/IEC 27005:2008, podría requerirse una o varias iteraciones sobre esta actividad, en busca de retroalimentación y redefiniciones. **Consideraciones:** Definir el criterio básico de evaluación de riesgo es una actividad de la norma ISO/IEC 27005:2008 que no es explícita en el método OCTAVE. El método OCTAVE no propone definir un criterio básico de evaluación de riesgo. Considera al impacto como componente principal para definir si se acepta o mitiga el riesgo y considera a la probabilidad como un criterio para determinar qué planes de mitigación implementar en primer lugar; la norma ISO/IEC 27005:2008 propone la definición del mencionado criterio. Para la priorización de riesgos, se ha optado por el criterio de evaluación de riesgos que propone la norma ISO 27005:2008 y

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
	no únicamente por la probabilidad como propone el método OCTAVE.
A2 Definir el criterio básico de impacto **A29** Creación de criterios de evaluación de riesgos	**Descripción de acoplamiento:** Consolidar esta actividad, definiendo el criterio básico de impacto por cada área de impacto, indicando lo que constituye un impacto alto, medio o bajo ó su correspondiente escala de acuerdo a la metodología de estimación del riesgo; con el propósito de que en base a esta definición se pueda establecer el valor del impacto. **Nombre de actividad acoplada:** Definir el criterio básico de impacto. **Ventaja:** Contar con el criterio de básico de impacto, previo a la evaluación de riesgos permite hacer uso y refinamiento de este desde la primera evaluación, adicionalmente facilitará el entendimiento de la valoración de impacto que se realizará en actividades posteriores. Adicionalmente permitirá enfocar la determinación del resto de criterios básicos y la metodología de estimación del riesgo, acorde a un enfoque común. **Desventaja:** Al ubicar esta actividad antes de las actividades de evaluación de riesgo, de acuerdo a lo que indica la norma ISO/IEC 27005:2008, podría requerirse una o varias iteraciones sobre esta actividad, en busca de retroalimentación y redefiniciones. **Consideraciones:** Para establecer el criterio básico de impacto se debe organizar por pareas de impacto sobre la base del contexto organizacional

Norma ISO/IEC 27005:2008 **Método OCTAVE**	**Oportunidad de acoplamiento**
	acerca de las pérdidas provocadas, esto de acuerdo a la propuesta del método OCTAVE; la norma ISO/IEC 27005:2008 hace una propuesta similar por lo que es necesario que la organización defina y priorice sus propias áreas de impacto.
A3 Definir el criterio básico de aceptación de riesgo	**Descripción de acoplamiento:** Mantener esta actividad como previa a la evaluación de riesgos, como lo propone la norma ISO/IEC 27005:2008. **Nombre de actividad acoplada:** Definir el criterio básico de aceptación de riesgo. **Ventaja:** Proporcionar desde un inicio del proceso, el conocimiento de cuando aceptar un riesgo, facilitará determinar el enfoque de tratamiento al riesgo mediante una comparación del riesgo estimado con el criterio de aceptación del riesgo. **Desventaja:** Al ubicar esta actividad antes de las actividades de evaluación de riesgo, de acuerdo a lo que indica la norma ISO/IEC 27005:2008, podría requerirse una o varias iteraciones sobre esta actividad, en busca de retroalimentación y redefiniciones. **Consideraciones:** Definir el criterio básico de aceptación de riesgo es una actividad de norma ISO/IEC 27005:2008 que no es explícita en el método OCTAVE, la aceptación o mitigación del riesgo en el método OCTAVE se basa en el impacto. Como se puede observar para el modelo propuesto, se ha optado por el enfoque de la norma ISO/27005:2008, pues la aceptación del riesgo se basa en el criterio de aceptación de riesgo y no únicamente en el impacto

Norma ISO/IEC 27005:2008 Método OCTAVE	Oportunidad de acoplamiento
	como lo propone el método OCTAVE.

Tabla 2.3-1 Oportunidades de acoplamiento entre la norma ISO/IEC 27005:2008 y el método OCTAVE

Fuente: Los autores

Las oportunidades de acoplamiento, completas, para todas las actividades, pueden encontrarse en el Anexo 3.

2.4 ESQUEMA DE ACOPLAMIENTO DE LA NORMA ISO/IEC 27005:2008 CON EL MÉTODO OCTAVE

De acuerdo a las oportunidades de acoplamiento detalladas en la sección anterior, a continuación se muestra el esquema de acoplamiento de la Norma ISO/IEC 27005:2008 con el Método OCTAVE, en base a sus actividades; los tipos de acoplamiento son (M) Mantener esta actividad, (C) Consolidar actividades, (N) No mantener la actividad.

No.	Norma ISO/IEC 27005:2008	Actividad acoplada	Tipo	Método OCTAVE
1		Preparación	M	Preparación
2		Obtener patrocinio de la alta dirección	M	Obtener patrocinio de la alta dirección para OCTAVE.
3		Seleccionar a los miembros del equipo de análisis	M	Seleccionar a los miembros del equipo de análisis
4	Definir el alcance Definir los límites	Definir el alcance	C	Seleccione las áreas operativas para participar en OCTAVE
5		Selección de los participantes	M	Selección de los participantes

No.	Norma ISO/IEC 27005:2008	Actividad acoplada	Tipo	Método OCTAVE
6		Coordinar la logística	N	Coordinar la logística
7	Determinar la metodología de estimación de riesgo	Determinar la metodología de estimación de riesgo	M	
8	Definir el criterio básico de evaluación de riesgo	Definir el criterio básico de evaluación de riesgo	M	
9	Definir el criterio básico de impacto	Definir el criterio básico de impacto	C	Creación de criterios de evaluación de riesgos
10	Definir el criterio básico de aceptación de riesgo	Definir el criterio básico de aceptación de riesgo	M	
11	Definir la organización para la gestión de riesgos de seguridad de la información	Definir la organización para la gestión de riesgos de seguridad de la información	M	
12	Identificación de activos	Identificar activos	C	Identificar los activos y las prioridades relativas. Selección de los activos críticos
13		Identificar las áreas de interés	M	Identificar las áreas de interés
14		Identificar los requisitos de seguridad	M	Identificar los requisitos de seguridad
15	Identificación de	Identificar controles	C	Capturar el

No.	Norma ISO/IEC 27005:2008	Actividad acoplada	Tipo	Método OCTAVE
	controles existentes.	existentes.		conocimiento de las prácticas actuales de seguridad y vulnerabilidades de la organización
16		La consolidación de información de los procesos de 1 a 3	N	La consolidación de información de los procesos de 1 a 3
17		Perfeccionamiento de los requisitos de seguridad para activos críticos	N	Perfeccionamiento de los requisitos de seguridad para activos críticos
18	Identificación de amenazas	Identificar amenazas	C	La identificación de las amenazas a los activos críticos
19		Seleccionar los componentes de la infraestructura a evaluar	M	Seleccionar los componentes de la infraestructura a evaluar
20	Identificación de vulnerabilidades	Identificar vulnerabilidades tecnológicas	C	Evaluación de componentes de infraestructura
21	Identificación de consecuencias	Identificar impacto (consecuencias)	C	Identificar y analizar los riesgos
22	Generar el listado de consecuencias (impacto para el negocio) valoradas	Valorar el impacto de las amenazas	C	La evaluación del impacto de las amenazas

No.	Norma ISO/IEC 27005:2008	Actividad acoplada	Tipo	Método OCTAVE
23	Describir la probabilidad de amenazas a los activos críticos	Describir la probabilidad de amenazas	M	
24		Definir el criterio de probabilidad	M	Crear criterios de probabilidad de la evaluación y evaluar (parcial)
25	Generar la valoración cuantitativa o cualitativa de la probabilidad de incidente.	Valorar la probabilidad de incidente	C	Crear criterios de probabilidad de la evaluación y evaluar (parcial)
26	Estimar el nivel del riesgo Evaluar el riesgo	Estimar (valorar) y priorizar el nivel de riesgo	C	Priorizando la mitigación de riesgo
27		Consolidar la información de los procesos 1, 2, y 3.	N	Consolidar la información de los procesos 1, 2, y 3.
28		Revisar los perfiles de riesgo	N	Revisar la información de riesgos
29		Crear una estrategia de protección	M	Crear una estrategia de protección
30	Reducción del riesgo Retención del riesgo Evitar los riesgos Transferencia de riesgos	Crear planes de mitigación	C	Crear planes de mitigación

No.	Norma ISO/IEC 27005:2008	Actividad acoplada	Tipo	Método OCTAVE
	Determinación del riesgo residual Aceptación del riesgo			
31		Crear lista de acciones	M	Crear lista de acciones
32		Preparar la presentación de tratamiento al riesgo	M	Preparar la reunión con la alta dirección
33		Revisar y perfeccionar la estrategia de protección	N	Revisar y perfeccionar la estrategia de protección
34		Crear los siguientes pasos	M	Crear los siguientes pasos
35	Comunicar el riesgo	Comunicar el riesgo	M	
36	Monitoreo y revisión de factores de riesgo	Monitorear y revisar los factores de riesgo	M	
37	Monitoreo, revisión y mejora de la gestión de riesgo	Monitorear, revisar y mejorar la gestión de riesgo	M	

Tabla 2.4-1 Esquema de acoplamiento de la norma ISO/IEC 27005:2008 con el Método OCTAVE

Fuente: Los autores

De acuerdo a la tabla anterior, se puede observar que el esquema de acoplamiento se ha completado con todas las actividades de la norma ISO/IEC 27005:2008 en adición a algunas actividades del método OCTAVE, que incluye aquellas que ambos modelos tienen en común. Adicionalmente al esquema de acoplamiento propuesto en la tabla anterior, se debe incorporar aquellos principios y atributos que parten del enfoque OCTAVE que dan soporte a las actividades propuestas por el método OCTAVE que son parte del esquema de acoplamiento. A continuación se detallan

estos principios y atributos y su justificación de aplicabilidad al esquema de acoplamiento:

Principio/Atributo	**Descripción**	**Aplicabilidad**
Principio 1 (seguridad)	La auto-dirección	Si, serán los miembros de la organización los que dirijan las actividades de la gestión de riesgos de seguridad de la información.
Principio 2 (seguridad)	Medidas adaptables	Si, el proceso de evaluación será adaptable a nuevas tecnologías y cambios.
Principio 3 (seguridad)	Proceso definido	Si, se definirá responsabilidades, actividades, herramientas, catálogos de evaluación.
Principio 4 (seguridad)	Fundación para un proceso continuo	Si, se institucionalizará las buenas prácticas de seguridad, haciéndolas rutinariamente.
Principio 1 (no exclusivo de seguridad)	Visión del futuro	Si, se gestionará la incertidumbre mediante la exploración de interrelaciones entre activos, amenazas y vulnerabilidades; examinando el impacto resultante en la misión y objetivos de negocio organizacionales.
Principio 2 (no exclusivo de seguridad)	Centrarse en focos críticos	Si, se centrará en los problemas de seguridad de la información más críticos.
Principio 3 (no exclusivo de seguridad)	Gestión Integrada	Si, las políticas y estrategias de seguridad serán coherentes con las políticas y estrategias organizacionales
Principio 1	Comunicación	Si, se apoyará la comunicación abierta

(organizacional y cultural)	abierta	de información sobre riesgos a través de un enfoque de gestión en colaboración
Principio 2 (organizacional y cultural)	Perspectiva global	Si, se consolidará perspectivas individuales para formar una imagen global de los riesgos de seguridad de información
Principio 3 (organizacional y cultural)	Trabajo en equipo	Si, el trabajo en equipo será interdisciplinario.
Atributo 1	Equipo de análisis (PSI1, POC3)	Si, este equipo gestionará, dirigirá las actividades de gestión de riesgo de seguridad de la información, será responsable de tomar decisiones
Atributo 2	Aumento de las habilidades de análisis del equipo (PSI1, POC3)	Si, se incluirá a más personas (internas o externas) que tengan habilidades o conocimientos específicos requeridos por el proceso
Atributo 3	Catálogo de prácticas (PSI2, PSI4)	Si, se considerará áreas de práctica estratégicas y operativas de seguridad coherentes con todo lineamiento que la organización debe cumplir, permitirá a una organización evaluarse a sí misma en contra de una medida conocida y aceptada, ofrecerá una base para la estrategia de protección y planes de mitigación
Atributo 4	Perfil de amenazas genéricas (PSI2)	Si se considerará una amplia gama de fuentes de amenazas potenciales a los activos críticos

Atributo 5	Catálogo de vulnerabilidades (PSI2)	Si, se considerará las debilidades tecnológicas actuales a ser evaluadas sobre los componentes clave de la infraestructura informática
Atributo 6	Actividades de evaluación definidas (PSI3)	Si, se considerará los procedimientos de preparación, alcance, actividad, herramientas, hojas de trabajo, catálogos de prácticas de evaluación de seguridad de la información definidos y documentados
Atributo 7	Resultados de evaluación documentados (PSI3)	Si, se incluirá riesgos a los activos críticos de la organización así como las estrategias y planes de seguridad
Atributo 8	Alcance de la evaluación (PSI3, PNS1)	Si, se incluirá pautas para ayudar a la organización a decidir qué unidades de negocio incluir en la evaluación
Atributo 9	Siguientes pasos (PSI4)	Si, se incluirá los pasos necesarios para implementar las estrategias y planes de seguridad.
Atributo 10	Participación de la alta directiva (PSI4, POC1)	Si, se requerirá el patrocinio y la participación activa de los altos directivos de la organización
Atributo 11	Enfoque al riesgo (PNS1)	Si, se incluirá el examen de las interrelaciones entre los activos, las amenazas a los activos y vulnerabilidades
Atributo 12	Actividades focalizadas (PNS2)	Si, se focalizará en los problemas críticos, a través de talleres para obtener información relacionada con la

		seguridad, actividades de análisis que utilizan información de los activos centrándose en la identificación de amenazas y riesgos, alcance, prioridades a través de la probabilidad e impacto.
Atributo 13	Aspectos organizacionales y tecnológicos (POC1, POC2)	Si, se incluirá las actuales prácticas de seguridad, vulnerabilidades, debilidades en los sistemas de tecnología de información.
Atributo 14	Participación de tecnología y negocio (POC1, POC2, POC3)	Si, participarán varios niveles de la organización.
Atributo 15	Enfoque colaborativo (POC3)	Si, se exigirá a todas las personas participantes colaborar en los talleres.

Tabla 2.4-2Principios y atributos del enfoque OCTAVE

Fuente: Los autores

De acuerdo al esquema de acoplamiento planteado, se puede observar lo siguiente:

Tipo de acoplamiento	**Cantidad de actividades**
Actividades comunes, consolidadas por la norma ISO/IEC 27005:2008 y el método OCTAVE (se mantienen).	11
Actividades no comunes, de la norma ISO/IEC 27005:2008 que se mantienen.	8
Actividades no comunes, del método OCTAVE que se mantienen.	12
Actividades no comunes, de la norma ISO/IEC 27005:2008 que no se mantienen.	0
Actividades no comunes, del método OCTAVE que no se	0

mantienen (6 actividades).	
	31

Tabla 2.4-3 Cantidad de actividades por modelo para el esquema de acoplamiento

Fuente: Los autores

A continuación se muestra la gráfica que muestra la distribución porcentual de actividades para el esquema de acoplamiento para el modelo:

Figura 2.4-1 Distribución porcentual de actividades fuera/dentro de esquema de acoplamiento por modelo

Fuente: Los autores

La norma ISO/IEC 27005:2008 proporciona todas sus actividades al modelo propuesto. Sin embargo, de acuerdo a la gráfica anterior se puede observar que el método OCTAVE proporciona más actividades al modelo que la norma, con porcentajes del 39% y 26% respectivamente, esto se debe a que el método OCTAVE tiene un nivel mayor de detalle que la norma, por tanto tiene también muchas más actividades. Finalmente, se pude observar que el 35% de actividades del modelo son comunes entre el método OCTAVE y la norma, lo que indica también que hay una afinidad considerable entre ambas propuestas de gestión de riesgos de seguridad de la información.

CAPÍTULO 3
DISEÑO DEL MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

3.1 INTRODUCCIÓN

El presente modelo tiene por objetivo proveer de lineamientos referenciales para llevar a cabo las actividades relacionadas a la de gestión de riesgos de seguridad de la información en una organización, no provee una metodología específica para la gestión de riesgos de seguridad de la información, pues le corresponde a cada organización ajustar su propio enfoque de gestión de riesgos de acuerdo a su propio contexto u objetivos específicos para su manejo de riesgos de seguridad de la información.

El acoplamiento de las actividades de gestión de riesgos de seguridad de la información propuestas por el método OCTAVE y las definidas por la norma ISO/IEC 27005:2008, son la base referencial sobre la que se ha establecido el presente modelo de gestión de riesgos de seguridad de la información.

El presente modelo está dirigido a directivos y personal involucrado en la gestión de riesgos de seguridad de la información.

3.1.1 ALCANCE

El presente modelo es aplicable a todo tipo de organización, y debe ser tomado como lineamientos referenciales para la gestión de riesgos de seguridad de su información.

3.2 MARCO CONCEPTUAL

3.2.1 TAXONOMÍA DEL RIESGO

La presente taxonomía tiene por objetivo permitir que los términos del modelo de gestión de riesgos de seguridad de la información sean precisos, de esta forma se

pueden entender de la misma manera por parte de los involucrados en las diferentes actividades.

A continuación se muestra una gráfica que detalla los componentes de la taxonomía de riesgos:

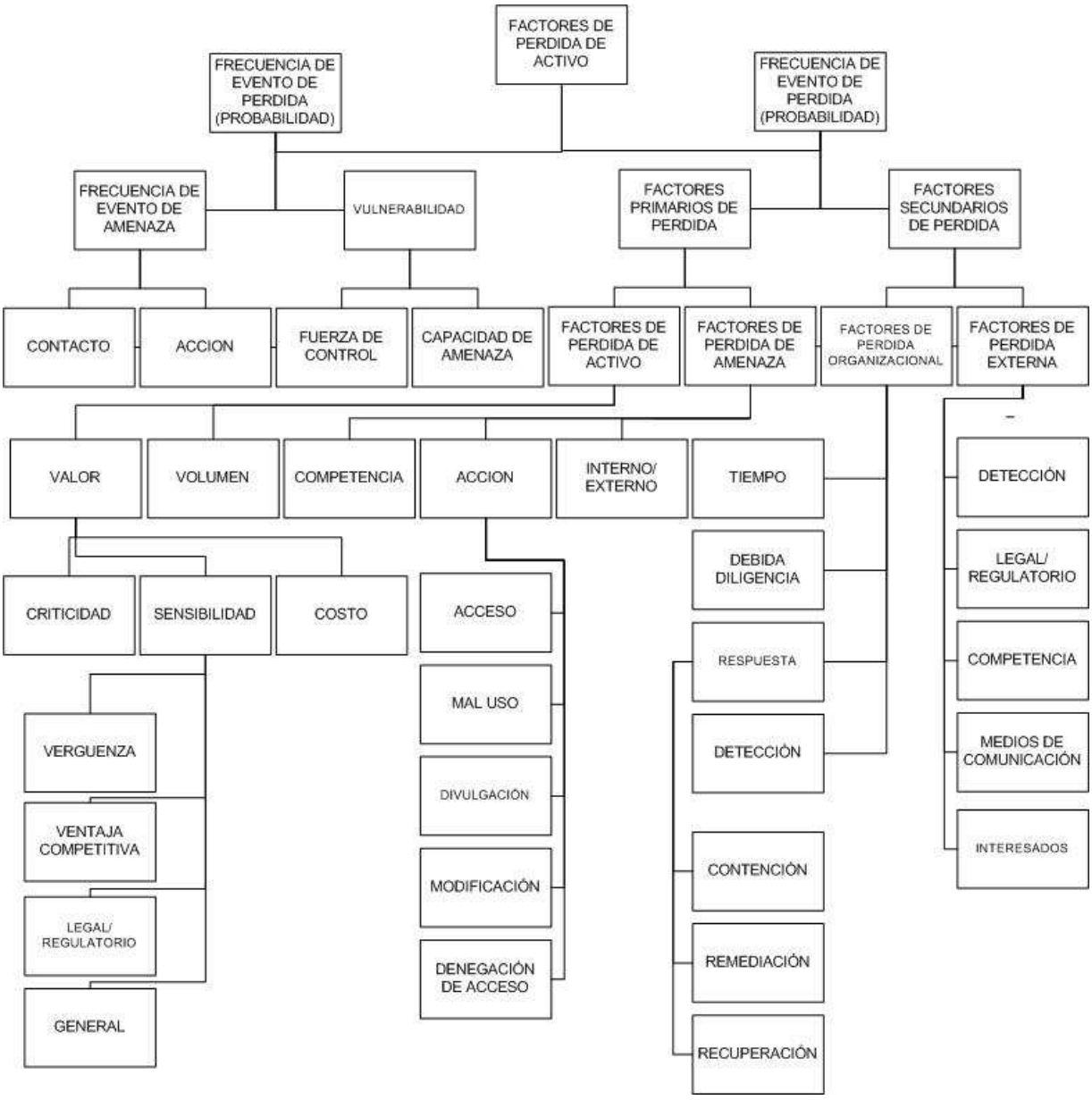


Figura 3.2-1 Taxonomía del riesgo

Fuente: The Open Group

En la gráfica anterior, se puede observar el árbol taxonómico de componentes de riesgo; a continuación se definen estos componentes:

Riesgo.- Es la probable frecuencia y probable magnitud de pérdida futura. Los componentes del riesgo son la probabilidad (probable frecuencia) e impacto (probable magnitud de pérdida futura).

Probabilidad (frecuencia de evento de pérdida).- Es la ocurrencia en un plazo en que un agente de amenaza puede infligir daño sobre un activo [7 pág. 12].

Frecuencia del evento de amenaza.- Es la ocurrencia en un plazo en que un agente actuará contra un activo [7 pág. 12]. Este componente no indica si el ataque fue exitoso.

Contacto.- Es la frecuencia probable en un plazo dado que un agente contactará a un activo. Puede ser físico o lógico (sobre la red) [7 pág. 13]. Puede ser de tipo regular, intencional o al azar.

Acción.- Es la probabilidad de que un agente actúe en contra de un activo mientras el contacto ocurre [7 pág. 13]. Depende de los siguientes factores: valor (para el agente de ejecutar el acto), nivel de esfuerzo (para el agente) y riesgo (probabilidad de consecuencias negativas para el agente).

Vulnerabilidad.- Es la probabilidad de que un activo sea inhabilitado a resistir acciones contra el agente de amenaza [7 pág. 14].

Capacidad de amenaza.- Es la capacidad probable de que un agente de amenaza sea capaz de aplicar contra un activo [7 pág. 15].

Fuerza de control.- Es la fuerza de un control comparada a la línea base de medida de fuerza. Es decir qué cantidad de fuerza es capaz de resistir el control [7 pág. 15]. Por ejemplo la fortaleza de una contraseña.

Impacto (magnitud de pérdida probable).- Es el resultado probable de un evento de amenaza [7 pág. 15]. Las formas de pérdidas podrían relacionarse a la

productividad, reemplazo de activos, multas y juicios, ventaja competitiva y reputación.

Factores primarios de impacto (pérdida):

Factores de pérdida de activos.- Se considera al valor (responsabilidad) y el volumen.

Valor (responsabilidad).- Tiene un rol importante en la naturaleza como en la magnitud de la pérdida, que puede definir mediante la criticidad (características de un activo que impactan la productividad), costo (valor intrínseco de un activo), sensibilidad (el daño que puede ocurrir de una revelación no intencionada). La sensibilidad puede involucrar la reputación (daño debido a la naturaleza de la información), ventaja competitiva (secretos comerciales), legales/regulatorios y general (el resto no determinadas).

Volumen.- Indica que más activos en riesgo iguala mayor magnitud de pérdida si un evento ocurre.

Factores de pérdida de amenazas.- Estos factores incluye la competencia (cantidad de daño que el agente es capaz de infligir), si el agente es interno/externo y las siguientes acciones sobre los activos: (acceso no autorizado), mal uso (uso no autorizado de activos), revelación (de información sensible), modificación (cambios no autorizados a un activo), negación de acceso (incluye la destrucción, robo).

Factores secundarios de impacto (pérdida).- Se refiere a aquellos organizacionales y características del ambiente externo que influencian la naturaleza y grado de la pérdida, que incluye:

Factores organizacionales de perdida.- Incluye, pero no se limita a al tiempo (el instante en que da el evento), la diligencia debida (si no existen las medidas preventivas razonables) y como la organización responde a un evento (contención, remediación y recuperación).

Factores externos de pérdida.- Generalmente, constan de las siguientes categorías como la detección (externa), el panorama legal/regulatorio (local, estatal o internacional), panorama competitivo (habilidad de la competencia de tomar ventaja), los medios y los interesados externos (los accionistas podrían llevarse el negocio a otro lado). Estos factores pueden resultar en formas de pérdidas directas (productividad, respuesta, reemplazo) debido a la criticidad y valor de los activos. Adicionalmente pueden presentar pérdidas secundarias debido a reacciones externas a eventos de pérdida. Todos estos factores pueden considerarse como reacciones a un evento.

3.2.2 TÉRMINOS Y DEFINICIONES EN GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Activo de información.- Datos, documentos físicos o electrónicos, propiedad intelectual utilizada en los procesos organizacionales.

Activo crítico.- Algo de mayor valor para la organización respecto al resto.

Actor.- Propiedad de una amenaza que define quien o que podría violar los requerimientos de seguridad (confidencialidad, integridad y disponibilidad) de un activo [4 pág. 293].

Área de interés.- Situación o escenario en los cuales alguien está preocupado de activos importantes [4 pág. 293].

Comité de seguridad de la información.- Es un ente organizacional generalmente conformado pero no limitado a representantes de las áreas de recursos humanos, tecnología de la información, área legal, oficial de seguridad de la información; que tiene por objetivo revisar, debatir toda temática de riesgos de seguridad de la información y de ser el intermediario entre la lata directiva y los interesados en cuanto a la comunicación continua del riesgo.

Comunicar el riesgo.- Intercambiar o compartir información acerca del riesgo entre los entes decidores y los interesados [2 pág. 2].

Confidencialidad.- Mantener la información privada e inaccesible a quien no tiene autorización de accederla.

Clases de componentes clave.- Categorías de dispositivos relevantes en la transmisión, almacenamiento y proceso de la información, asociados a aquellos componentes sobre los cuales se pretende realizar un análisis de vulnerabilidades tecnológicas.

Criterio de evaluación.- Medidas sobre las cuales un riesgo toma valor, en base a una comparación.

Destrucción.- Eliminación de un activo, sin posibilidad de reconstruirle.

Disponibilidad.- Grado o frecuencia a la cual un activo debe estar listo para utilizarse [4 pág. 294].

Gestión de riesgos de seguridad de la información.- La gestión de riesgos de seguridad de la información es el proceso de identificar riesgos e implementar planes para hacerles frente [1 pág. 295].

Enfoque de mitigación.- Se refiere a como la organización va a manejar el riesgo, se puede aceptarlo o mitigarlo. Dentro de la mitigación, se puede evitarlo, transferirlo o reducirlo.

Equipo de análisis.- Equipo interdisciplinario que conduce la gestión de riesgos de seguridad de la información.

Estimar el riesgo.- Proceso de asignar valores de probabilidad y consecuencia al riesgo [2 pág. 2].

Evitar el riesgo.- Decisión de no involucrarse, no tomar acción o retirarse de una situación de riesgo [2 pág. 2].

Identificación del riesgo.- Proceso de encontrar, listar y caracterizar elementos del riesgo [2 pág. 2].

Integridad.- Autenticidad, exactitud y completitud de un activo [4 pág. 296].

Interrupción.- Alterar la disponibilidad de un activo.

Lista de acciones.- Lista de acciones específicas que las personas de una organización pueden llevar a cabo sin necesidad de entrenamiento especializado ni cambios de políticas, etc. [4 pág. 293].

Mitigar.- Implementar acciones para contrarrestar las amenazas asociadas a un riesgo.

Modificación.- Alterar un activo de forma no autorizada.

Perfil de amenaza.- Definición de un rango de amenazas que pueden afectar a un activo. Contiene categorías agrupadas de acuerdo a las fuentes de amenaza (actores humanos con acceso a la red, actores humanos con acceso físico, problemas de sistemas y otros problemas) [4 pág. 299].

Perfil de riesgo.- Definición de un rango de riesgos que pueden afectar a un activo. Contiene categorías agrupadas de acuerdo a las fuentes de amenaza (actores humanos con acceso a la red, actores humanos con acceso físico, problemas de sistemas y otros problemas) [4 pág. 298].

Perfil genérico de riesgo.- Catálogo que contiene un rango de todos los riesgos potenciales bajo consideración [4 pág. 295].

Plan de mitigación de riesgo.- Plan direccionado a mitigar el riesgo, bajo los enfoques de reducir, transferir o evitarlo.

Práctica de seguridad.- Acciones dirigidas a gestionar la seguridad de la información.

Práctica estratégica.- Prácticas de la seguridad de la información a nivel de políticas organizacionales.

Reducción del riesgo.- Acciones tomadas para reducir la probabilidad, consecuencias negativas o ambas, respecto al riesgo.

Requerimientos de seguridad.- Cualidades de los activos de información, incluye la confidencialidad, integridad y disponibilidad.

Retención del riesgo.- Aceptación de la carga de riesgo o el beneficio obtenido de un riesgo particular [2 pág. 2].

Revelación.- Acceso no autorizado a información confidencial.

Resultados.- Resultado de una posible amenaza: revelación, modificación, destrucción interrupción.

Sistema.- Grupo lógico de componentes diseñados para realizar funciones definidas para alcanzar objetivos definidos [4 pág. 299].

Sistema de activos.- Sistemas de información que procesan y almacenan información. Son una combinación de activos de información, software, y hardware. Cualquier host, cliente, o servidor puede ser considerado un sistema [4 pág. 299].

Sistema de interés.- Sistema que está más íntimamente relacionado al activo crítico [4 pág. 299].

Transferencia del riesgo.- Compartir con otra parte la carga del riesgo o el beneficio obtenido de un riesgo [2 pág. 2].

Valor esperado.- Valor resultante de multiplicar el valor de probabilidad por el valor de impacto.

Vulnerabilidad organizacional.- Debilidad en la política o práctica organizacional que puede resultar en la ocurrencia de acciones no autorizadas [4 pág. 297].

3.3 ESTRUCTURA

3.3.1 ASPECTOS GENERALES

El modelo se basa en un conjunto de procesos que se componen de actividades. El desarrollo de estas actividades se basará en la ejecución de talleres. Los participantes en los talleres de cada una de las actividades, dependiendo de la naturaleza de estas, pueden ser el equipo de análisis o miembros de las áreas involucradas establecidas en el alcance. Este equipo de análisis se encargará de la revisión, consolidación de la información generada en los talleres por parte de los participantes de las áreas involucradas. El equipo de análisis se define de forma inicial, así como los participantes de los talleres, sin embargo la asignación de estos últimos es dinámica e incluso podría requerir la participación de expertos en ámbitos específicos de seguridad de la información, de ser el caso.

Las actividades de forma referencial, se definen como secuenciales es decir, se ejecutan una después de otra, a excepción de la comunicación y monitoreo del riesgo que son actividades transversales a todo el modelo; sin embargo, debido a la complejidad de la naturaleza de la gestión de riesgos de seguridad de la información, podría ser necesaria retroalimentación, es decir se podrían formar bucles que requieran regresar a redefinir actividades anteriores, estas iteraciones deben tender a ser tan pocas como sea posible; es decir cuando sea estrictamente necesario.

Para apalancar la ejecución de las actividades del modelo de gestión de riesgos de seguridad de la información, se considerará aplicar a través de las actividades planteadas, los enfoques que a continuación se muestran:

La auto-dirección.- Serán los miembros de la organización los que dirijan las actividades de la gestión de riesgos de seguridad de la información.

Medidas adaptables.- El proceso de gestión de riesgos de seguridad de la información será adaptable a nuevas tecnologías y cambios

Proceso definido.- Se definirá responsabilidades, actividades, herramientas, catálogos.

Fundación para un proceso continuo.- Se Institucionalizará las buenas prácticas de seguridad, haciéndolas rutinariamente.

Visión del futuro.- Se gestionará la incertidumbre mediante la exploración de interrelaciones entre activos, amenazas y vulnerabilidades; examinando el impacto resultante en la misión y objetivos de negocio organizacionales.

Centrarse en focos críticos.- Se centrará en los problemas de seguridad de la información más críticos.

Gestión Integrada.- Las políticas y estrategias de seguridad serán coherentes con las políticas y estrategias organizacionales.

Comunicación abierta.- Se apoyará la comunicación abierta de información sobre riesgos a través de un enfoque de gestión en colaboración.

Perspectiva global.- Se consolidará perspectivas individuales para formar una imagen global de los riesgos de seguridad de información.

Trabajo en equipo.- El trabajo en equipo será interdisciplinario.

3.3.2 COMPONENTES ESTRUCTURALES

La gestión de riesgos de seguridad de la información, consiste de un conjunto de procesos que se conforman de actividades, a continuación se puede observar una gráfica explicativa al respecto:

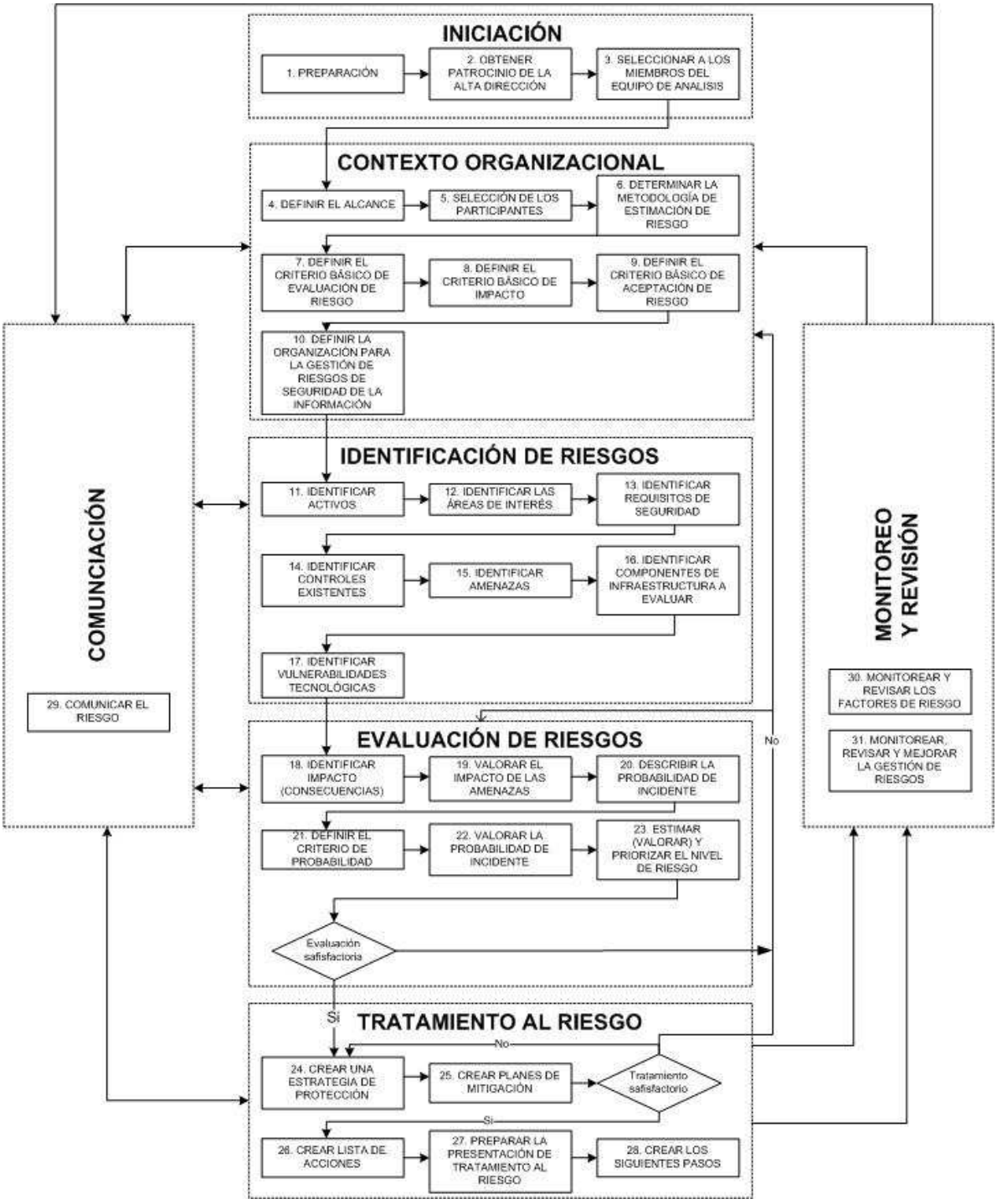


Figura 3.3-1 Modelo de gestión de riesgos de seguridad de la información

Fuente: Los autores

Como se puede observar en el esquema mostrado en la figura anterior, la gestión de riesgos de seguridad de la información empieza con un proceso de iniciación, donde surge la iniciativa de realizar acciones enfocadas a la gestión de riesgos de seguridad de la información apalancándose en el apoyo de la alta directiva organizacional, en este punto se definirá el comité de seguridad de la información; para posteriormente definir el equipo que realizará las tareas de análisis del conocimiento obtenido en los respectivos talleres.

A continuación se definirá el contexto propio de la organización desde una perspectiva de gestión de riesgos de seguridad de la información, que incluye las especificaciones del alcance, la elección de los participantes en los talleres de trabajo, la determinación de la metodología de estimación de riesgo, los criterios contra los que se evaluará el riesgo, se medirá y aceptará el impacto y la definición de la organización que gestionará los mencionados riesgos.

Posteriormente, se ejecutará un proceso de identificación de riesgos en la organización, a partir de la identificación de los activos más importantes de acuerdo al alcance, se identificará las áreas de interés, requisitos de seguridad y controles existentes para cada activo. Luego, se identificará las amenazas a partir de las áreas de interés, tomando como ayuda los perfiles de amenaza genéricos. Finalmente, en este proceso realizará la selección y posterior evaluación de componentes tecnológicos, con el propósito de detectar las vulnerabilidades tecnológicas y las recomendaciones para tratarlas. Se debe incluir en el contexto de esta evaluación a los componentes tecnológicos relacionados a los activos críticos.

Una vez identificados los riesgos de seguridad de la información, se los evalúa, a través de la identificación y valoración del impacto (consecuencia de un evento) y de la probabilidad de incidente. En este punto, se debe aplicar la metodología de estimación del riesgo en conjunto con el criterio básico de impacto de acuerdo a obtener el nivel de estimación del riesgo.

Adicionalmente, si es que la evaluación de riegos no ha generado la suficiente información para determinar el tratamiento al riesgo, entonces será necesaria otra

iteración sobre la definición del contexto organizacional. Caso contrario, se procede a determinar el tratamiento al riesgo, donde se define los lineamientos globales de protección a través de una estrategia de protección, posteriormente se establecerá los planes de mitigación en base al enfoque de riesgo (aceptar/mitigar). En caso de no llegar a un nivel de riesgo aceptable, será necesaria otra iteración a la evaluación de riesgo. Caso contrario, se determinará la lista de acciones a corto plazo y sin mayor requerimiento de entrenamiento, que pueden aplicarse para tratar el riesgo. A partir de esto, se preparará una presentación para la alta directiva al respecto de los puntos clave de los riesgos y las soluciones propuestas. Finalmente se generará los siguientes pasos, es decir, información importante para aterrizar, apalancar e implementar la estrategia, plan y acciones.

El modelo de gestión de riesgos, se apalanca sobre dos procesos que se ejecutan de forma transversal a todo el modelo, son los procesos de comunicación y; monitoreo y revisión del riesgo. El proceso de monitoreo del riesgo, se enfoca en que el riesgo debe ser continuamente comunicado y entendido entre los entes de decisión y los interesados, a través del comité de seguridad de la información. Finalmente, el proceso de monitoreo y revisión de riesgos se encarga de monitorear tanto los factores de riesgo como la mejora la gestión de los riesgos, esto debido a que el riesgo y sus factores no son estáticos, permitiendo de esta forma mantener una imagen general del riesgo a través del tiempo, asegurando que los planes son los adecuados de acuerdo al contexto y que existen los recursos necesarios para llevarlos a cabo.

3.3.3 RECURSOS DOCUMENTALES ADICIONALES

Con el propósito de ejecutar las actividades del modelo de gestión de riesgos de seguridad de la información, se requiere los siguientes recursos documentales adicionales:

- Catálogo de prácticas (que ayudan a gestionar la seguridad de la información en una organización). Se utilizará de forma referencial el proporcionado por la

norma ISO/IEC 27002:2005, considerando los dominios que aplique para el efecto.

- Catálogo de amenazas (lista de amenazas conocidas), el requisito es que sea un catálogo actualizado. Se utilizará de forma referencial el proporcionado por la norma ISO/IEC 27005:2008 en su Anexo E.
- Catálogo de vulnerabilidades, el requisito es que sea un catálogo actualizado. Se utilizará de forma referencial el proporcionado por la norma ISO/IEC 27005:2008 en su Anexo D.

3.4 DEFINICIÓN DE PROCESOS, ACTIVIDADES Y RECOMENDACIONES DE IMPLEMENTACIÓN

A continuación se muestra a detalle la especificación de cada uno de los procesos y sus correspondientes actividades dentro del modelo de gestión de riesgos de seguridad de la información.

3.4.1 PROCESO DE INICIACIÓN

El proceso de iniciación establece las actividades relacionadas al surgimiento de la iniciativa de realizar acciones enfocadas a la gestión de riesgos de seguridad de la información, apalancándose en el apoyo de la alta directiva organizacional y en la conformación del comité de seguridad de la información, para posteriormente definir el equipo que realizará las tareas de análisis del conocimiento obtenido en los respectivos talleres.

3.4.1.1 Actividad 1: Preparación

3.4.1.1.1 Detalle de actividad

Un miembro de la organización para la gestión de riesgos de seguridad de la información se auto-determinará coordinador. Este coordinador propiciará que surja la idea de iniciar acciones orientadas a la gestión de riegos de seguridad de la información.

El coordinador designará al personal que le apoyará en la logística organizativa de los recursos para llevar a cabo los talleres y en la documentación de la información obtenida.

Finalmente definirá un cronograma para la implementación del modelo.

3.4.1.1.2 Resultados

- Coordinador, personal de logística y documentación seleccionados. A continuación se muestra una plantilla de ayuda:

Resultados de actividades de preparación	
Definición de personal	
Coordinador de implementación	
Apellido	
Nombre	
Cargo	
Unidad Organizacional	
Personal de logística	
Apellido	
Nombre	
Cargo	
Unidad Organizacional	
Personal de documentación	
Apellido	
Nombre	
Cargo	
Unidad Organizacional	
Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-1 Actividades de preparación

Fuente: Los autores

- Cronograma.

3.4.1.1.3 Recomendaciones de implementación

El coordinador debería ser una persona miembro de la organización para la gestión de riegos de seguridad de la información, de preferencia con conocimiento en gestión de riesgos de seguridad de la información, de este modo se facilita la comprensión del modelo propuesto y se evita recursos destinados a extensas capacitaciones al respecto de la temática.

3.4.1.1.4 Fuentes

Modelo de gestión de riesgos de seguridad de la información.

3.4.1.2 Actividad 2: Obtener patrocinio de la alta dirección

3.4.1.2.1 Detalle de actividad

El coordinador, realizará lo siguiente:

- Trabajar con altos directivos de la organización para obtener el patrocinio para la implementación del modelo de gestión de riesgos de seguridad de la información.
- Concientizar a los altos directivos de que la seguridad de la información no es solamente un problema de tecnología de la información, sino organizacional.
- Coordinar y definir la conformación del comité de seguridad de la información, que será el ente que coordinará la comunicación entre los interesados y quienes toman las decisiones en la organización (alta directiva). Este comité también debatirá acerca del riesgo, su priorización, aceptación, y tratamiento.

3.4.1.2.2 Resultados

Patrocinio de la alta dirección. A continuación se muestra una plantilla de ayuda:

Resultado de patrocinio de la alta dirección		
Asistentes a la reunión		
Apellido	Nombre	Cargo
Puntos tratados y acuerdos		
Observaciones		
Fecha		
Realizado por		

Plantilla 3.4-2 Patrocinio de la alta dirección

Fuente: Los autores

3.4.1.2.3 Recomendaciones de implementación

Planificar y llevar a cabo una reunión con los altos directivos organizacionales, presentado un esquema muy conciso y claro acerca de la implementación del modelo de gestión de riesgos de seguridad de la información, enfocándose en los beneficios esperados para la organización y el camino a recorrer para lograrlo.

Se recomienda conformar el comité de seguridad de la información con representantes de recursos humanos, el área legal, área de tecnología de la información y el oficial de seguridad de la información.

3.4.1.2.4 Fuentes

Modelo de gestión de riesgos de seguridad de la información, plan estratégico organizacional

3.4.1.3 Actividad 3: Seleccionar a los miembros del equipo de análisis

3.4.1.3.1 Detalle de actividad

El coordinador, realizará lo siguiente:

- Componer el núcleo del equipo de análisis tomando como referencia al área de seguridad de la información de la organización, considerando personas de las unidades de negocio de la organización y al menos un miembro del departamento de tecnología de la información que tenga familiaridad con cuestiones de seguridad de la información.
- Familiarizar al equipo de análisis con el modelo de gestión de riesgos de seguridad de la información, pues serán estos los que lleven a cabo las actividades de análisis de la información obtenida en los talleres con los participantes de la organización.

3.4.1.3.2 Resultados

Equipo de análisis conformado. A continuación se muestra una plantilla de ayuda:

Selección de miembros del equipo de análisis			
Equipo de análisis			
Apellido	Nombre	Cargo	Unidad Organizacional
Observaciones			
Fecha			
Realizado por			

Plantilla 3.4-3 Selección de miembros del equipo de análisis

Fuente: Los autores

3.4.1.3.3 Recomendaciones de implementación

Generar un acta donde los miembros de este equipo firmen el comprometimiento a llevar a cabo las actividades de análisis requeridas por el modelo de gestión de riesgos de seguridad de la información.

3.4.1.3.4 Fuentes

Orgánico funcional organizacional.

3.4.2 PROCESO DE DEFINICIÓN DEL CONTEXTO ORGANIZACIONAL

El proceso de definición del contexto organizacional se lo establecerá de acuerdo a la naturaleza propia de la organización y sus necesidades específicas acorde a una perspectiva de gestión de riesgos de seguridad de la información, que incluye las especificaciones del alcance, la elección de los participantes en los talleres de trabajo, la determinación de la metodología de estimación de riesgo, los criterios contra los que se evaluará el riesgo, se medirá y aceptará el impacto y la definición de la organización que gestionará los mencionados riesgos.

3.4.2.1 Actividad 4: Definir el alcance

3.4.2.1.1 Detalle de actividad

El equipo de análisis realizará lo siguiente:

- Definir el alcance, guiando a la alta directiva en la elección de los procesos sobre los cuales se identificaran las áreas operativas a examinar. Se debe considerar entre las zonas operativas a tecnología de información. Hay que asegurar que los activos importantes serán tomados en cuenta.

3.4.2.1.2 Resultados

Alcance. A continuación se muestra una plantilla de ayuda:

Resultados de definición de alcance	
Detalle de alcance	
Macro proceso	
Proceso	
Áreas involucradas	
Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-4 Definición del alcance

Fuente: Los autores

3.4.2.1.3 Recomendaciones de implementación

Revisar los organigramas organizacionales, así como la documentación de los procesos y subprocesos en busca de definir a detalle las áreas operativas que se incluirá en el alcance. Al implementar por primera vez el modelo, se recomienda elegir un proceso importante parte de la cadena de valor del negocio incluyendo sus áreas operativas, pues para posteriores implementaciones se puede elegir otros procesos de la cadena de valor, para finalmente referirse a los procesos de apoyo.

Establecer formalmente el alcance en un acta que suscriban los miembros del equipo de análisis y la alta directiva.

3.4.2.1.4 Fuentes

Plan estratégico organizacional.

3.4.2.2 Actividad 5: Selección de los participantes

3.4.2.2.1 Detalle de actividad

El equipo de análisis realizará lo siguiente:

- Seleccionar a los participantes para los talleres posteriores, eligiendo de acuerdo al criterio de la alta directiva y mandos medios, a aquellos que cuenten con la mayor experiencia y conocimiento en el proceso al que el alcance se refiere. Hay que asegurarse de que ninguna información discutida

en un taller se atribuye a un individuo específico. En cualquiera de las actividades es posible incluir participantes de tal forma de asegurar las actividades necesarias para llevarlas a cabo.

- Capacitar a los participantes en el modelo de gestión de riesgos de seguridad.

3.4.2.2.2 Resultados

Participantes seleccionados. A continuación se muestra una plantilla de ayuda:

Resultados de selección de participantes			
Detalle de participantes			
Apellidos	Nombres	Área operativa	Tipo (Principal/Alterno)
Observaciones			
Fecha			
Realizado por			

Plantilla 3.4-5 Selección de participantes

Fuente: Los autores

3.4.2.2.3 Recomendaciones de implementación

Establecer formalmente los participantes para los talleres de las actividades posteriores, en un acta que suscriban los miembros del equipo de análisis y la alta directiva. Establecer los participantes con un esquema de principal y respaldo, siendo el de respaldo, quien asistirá a los talleres en caso de que el principal, bajo algún motivo no lo pueda hacer.

3.4.2.2.4 Fuentes

Orgánico funcional organizacional.

3.4.2.3 Actividad 6: Determinar la metodología de estimación de riesgo

3.4.2.3.1 Detalle de actividad

El equipo de análisis realizará lo siguiente:

- Definir la escala de valoración de probabilidad e impacto, basándose en un enfoque cuantitativo, cualitativo o una combinación.

- Determinar la metodología de estimación de riesgo, generando el esquema de valoración del riesgo en base a las escalas de probabilidad e impacto, considerando el enfoque cuantitativo, cualitativo o una combinación acorde a estas escalas.
- Considerar que la definición de una escala cualitativa (por ejemplo: alto, medio, bajo) únicamente indica que un valor es mayor o menor en comparación con otro. Mientras que una escala cuantitativa indica por cuanto un valor es mayor o menor en comparación con otro. Para el caso de una escala cuantitativa son necesarios datos históricos con los que no siempre se cuenta, depende también de la calidad del modelo; mientras que una escala cualitativa es fácil de entender pero conlleva la subjetividad inherente a la elección, aún cuando es necesario tomar en cuenta todo criterio objetivo con el que se cuente.
- Se recomienda en primera instancia un enfoque cualitativo para obtener la visión general del nivel de riesgo y revelar los mayores riesgos. Posteriormente podría ser necesario hacer un análisis más específico cuantitativo en los mayores riesgos.
- Considerar que, generalmente es menos complejo realizar un análisis cualitativo que hacer uno cuantitativo.
- Para valorar el riesgo, tanto para un enfoque cualitativo como para uno cuantitativo, se podría utilizar el valor esperado; para el caso de una valoración cualitativa se puede utilizar una matriz de valor esperado, mientras que para una valoración cuantitativa se puede utilizar un cálculo matemático, por ejemplo en base a la multiplicación de la probabilidad e impacto. Sin embargo, existen otras alternativas, que pueden observar en las recomendaciones de implementación.
- Considerar que la metodología de estimación de riesgo puede tener varios enfoques, y es la organización quien decide personalizar su forma de estimar el riesgo. Sin embargo, la metodología de estimación de riesgo, siempre debe estar definida a acorde a los criterios básicos de evaluación de riesgo, impacto

y aceptación de riesgo, que se definirán posteriormente; por lo que cualquier cambio en cualquiera de estas actividades, debe ser obligatoriamente revisado en las otras, en busca de posibles re-definiciones.

- La metodología de estimación de riesgo debe ser aprobada por la alta directiva.

3.4.2.3.2 Resultados

Metodología de estimación de riesgo. A continuación se muestra una plantilla de ayuda:

Resultados de determinar la metodología de estimación del riesgo			
Metodología de estimación del riesgo			
Enfoque	{cualitativo, cuantitativo, combinación}		
Justificación			
Escala de probabilidad			
Escala de impacto			
Estimación del riesgo en base a			
{detalle de la metodología}			
Observaciones			
Fecha			
Realizado por			

Plantilla 3.4-6 Determinar la metodología de estimación del riesgo

Fuente: Los autores

3.4.2.3.3 Recomendaciones de implementación

Para casos de organizaciones en las que se tiene evaluaciones previas de riesgos de seguridad de la información, se tiene experiencia acerca de estas, o se cuenta con datos históricos, es recomendable definir las escalas de estimación tomando como parámetro aquellas con las que ya se cuenta, o los datos históricos con los que se cuente. Por el contrario, para casos de organizaciones en las que no se tiene evaluaciones previas de riesgos de seguridad de la información, no se tiene

experiencia acerca de estas, o no se cuenta con datos históricos, es recomendable utilizar escalas cualitativas tanto para la probabilidad como para el impacto.

A continuación se muestran varios ejemplos de metodologías de estimación de riesgo:

Ejemplo 1

Metodología de estimación de riesgos basada en un enfoque cualitativo, haciendo referencia a lo propuesto por el método OCTAVE:

Escalas de impacto: Alto, Medio, Bajo

Escalas de probabilidad: Alta, Media, Baja

Matriz de valor aperado (enfoque cualitativo):

		Probabilidad		
		Alta	**Media**	**Baja**
Impacto	**Alto**	Alto	Alto	Medio
	Medio	Alto	Medio	Bajo
	Bajo	Medio	Bajo	Bajo

Tabla 3.4-1 Matriz de valor esperado (enfoque cualitativo)

Fuente: Método OCTAVE

Como se puede ver en la tabla anterior, el nivel del riesgo estimado (valor esperado), se refleja en el cruce de los valores correspondientes a las escalas de probabilidad e impacto.

En este enfoque se debe tener especial cuidado al analizar una valor esperado Medio, pues podría provenir de un impacto alto con probabilidad baja ó de impacto bajo con probabilidad alta; estos dos criterios deberían ser tratados de diferente manera.

Ejemplo 2

A continuación se muestra una metodología de estimación de riesgo con un enfoque cuantitativo, acorde al Anexo E de la norma ISO 27005:2008.

Escalas de impacto (definidas por el criterio básico de impacto): 1, 2, 3, 4, 5

Probabilidad (definida por la metodología de estimación de riesgo): 1, 2, 3, 4, 5

Amenaza	**Impacto**	**Probabilidad**	**Valor esperado = Impacto x Probabilidad**	**Ranking de amenaza**
Amenaza A	5	2	10	2
Amenaza B	2	4	8	3
Amenaza C	3	5	15	1
Amenaza D	1	3	3	5
Amenaza E	4	1	4	4
Amenaza F	2	4	8	3

Tabla 3.4-2 Matriz de estimación de riesgo (enfoque cuantitativo)

Fuente: Norma ISO/IEC 27005:2008

Como se puede observar en el cuadro anterior, el valor esperado para cada amenaza se obtiene de multiplicar la probabilidad y el impacto, mientras que el ranking es el orden respecto de acuerdo ordenamiento descendente del valor esperado.

Ejemplo 3

A continuación se muestra una metodología de estimación de riesgo con un enfoque combinado, acorde al Anexo E de la norma ISO 27005:2008.

Escalas de impacto (definidas por el criterio básico de impacto): muy bajo, bajo, medio, alto, muy alto

Probabilidad (definida por la metodología de estimación de riesgo): muy bajo, bajo, medio, alto, muy alto.

El esquema que a continuación se muestra debe aplicarse a cada amenaza.

	Probabilidad	Muy Baja	Baja	Media	Alta	Muy Alta
Impacto	Muy Bajo	0	1	2	3	4
	Bajo	1	2	3	4	5
	Medio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muy Alto	4	5	6	7	8

Tabla 3.4-3 Matriz de valor esperado (enfoque cuantitativo)

Fuente: Norma ISO/IEC 27005:2008

De acuerdo al cuadro anterior, se podría establecer la siguiente escala de riesgo:

Riesgo bajo: 0-2.

Riesgo medio: 3-5.

Riesgo alto: 6-8.

3.4.2.3.4 Fuentes

Información relevante acerca de análisis de riesgo en la organización, resultados de evaluaciones anteriores de riesgos de seguridad de la información.

3.4.2.4 Actividad 7: Definir el criterio básico de evaluación de riesgo

3.4.2.4.1 Detalle de actividad

El equipo de análisis realizará lo siguiente:

- Definir el criterio que permitirá priorizar el riesgo, a partir de su comparación con el riesgo estimado, se considerará referencialmente los siguientes criterios: al valor estratégico de los procesos del negocio, la criticidad de los activos de información, requerimientos legales y contractuales, expectativas y percepción de los interesados y consecuencias negativas en la reputación.

- Considerar que los criterios tomados en cuenta para la creación del criterio de evaluación del riesgo, pueden variar de acuerdo a la naturaleza de las organizaciones.
- Considerar que el criterio básico de evaluación del riesgo debe ser aprobado por la alta directiva, cada organización define su escala y se aplica en toda ella; esta escala debe definirse acorde a la metodología de estimación del riesgo.

3.4.2.4.2 Resultados

Criterio básico de evaluación del riesgo. A continuación se muestra una plantilla de ayuda:

Resultados de definición de criterio básico de evaluación de riesgo			
	Escala de estimación de riesgo		
Criterio	**Bajo**	**Medio**	**Alto**
Valor estratégico de los procesos del negocio			
Requerimientos legales y contractuales			
Expectativas y percepción de los interesados			
Observaciones			
Fecha			
Realizado por			

Plantilla 3.4-7 Definición de criterio básico de evaluación de riesgo

Fuente: Los autores

3.4.2.4.3 Recomendaciones de implementación

El criterio de evaluación de riesgo se define en base a la escala del riesgo estimado, de acuerdo a lo que determine la metodología de estimación de riesgo. Para cada criterio y por cada escala se recomienda definir descripciones narrativas de lo que implicada cada una de ellas, a modo de ejemplo a continuación se detalla un esquema referencial:

	Escala de estimación de riesgo		
Criterio	**Bajo**	**Medio**	**Alto**
Valor estratégico de	Los procesos de bajo valor estratégico de	Los procesos de mediano valor	Los procesos de alto valor

los procesos de información de negocio	negocio para la organización son los asociados a instalaciones.	estratégico de negocio para la organización son los asociados a atención al cliente.	estratégico de negocio para la organización son los asociados a facturación y cobro de planillas
…	…	..	..

Tabla 3.4-4 Ejemplo de criterio de evaluación de riesgo

Fuente: Los autores

3.4.2.4.4 Fuentes

Planes estratégico organizacional, información relevante de la organización.

3.4.2.5 Actividad 8: Definir el criterio básico de impacto

3.4.2.5.1 Detalle de actividad

El equipo de análisis realizará lo siguiente:

- Definir lo que constituye un impacto (consecuencia) alto, medio y bajo (o su escala equivalente acorde a la metodología de estimación del riesgo) para cada área de impacto (confianza del cliente, financiera, productividad, seguridad y salud, multas y penalidades legales, etc.), en base a la comprensión de los límites de riesgo ya existentes de la organización sobre la base de planes estratégicos y operativos, la responsabilidad, y las cuestiones relacionadas con el aseguramiento. Esto permitirá valorar las consecuencias (impacto al negocio que provocan pérdida de confidencialidad, integridad y disponibilidad de la información), se especifica de acuerdo al daño o costo para la organización a causa de un evento de seguridad de la información.
- Considerar que, las áreas de impacto, deben ser elegidas de acuerdo a la importancia que tengan en relación al negocio.
- Considerar que para cada organización puede aplicar áreas de impacto diferentes a las recomendadas por las mejores prácticas, de igual forma

algunas áreas recomendadas por las mejores prácticas puede no aplicar para cada organización.

- Considerar que, el criterio básico de impacto, así como las áreas de impacto elegidas y priorizadas, deben ser aprobadas por la alta directiva y se aplican a toda la organización.

3.4.2.5.2 Resultados

Criterio básico de impacto. A continuación se muestra una plantilla de ayuda:

Resultado de definición de criterio básico de impacto			
Área de Impacto 1			
Área de Impacto	Baja	Media	Alta
…			
Área de impacto 2			
Área de Impacto	Baja	Media	Alta
…			
Observaciones			
Fecha			
Realizado por			

Plantilla 3.4-8 Definición de criterio básico de impacto

Fuente: Los autores

3.4.2.5.3 Recomendaciones de implementación

Podría ser necesario realizar una priorización de áreas de impacto, que sería útil al considerar una escala cuantitativa de valoración de impacto, en este caso se recomienda utilizar una escala numérica, como referencia el siguiente esquema para ejemplificación:

Área de Impacto	**Prioridad (Importancia)**
Imagen y confianza del cliente	1
Financiera	2
Productividad	3
…	…

Tabla 3.4-5 Ejemplo de priorización de áreas de impacto

Fuente: Los autores

De acuerdo a establecer cada criterio básico de impacto, se recomienda definir narraciones descriptivas por cada escala, utilizando como referencia el siguiente esquema para ejemplificación (utilizando un enfoque cualitativo):

Área de impacto (Imagen y confianza del cliente)	**Alto**	**Medio**	**Bajo**
Confianza	Más de 30% de pérdida de confianza de cliente.	Del 10% al 30% de pérdida de confianza de cliente.	Menos del 10% de pérdida de confianza de cliente.
Imagen	…	…	…
….	…	…	…
…	…	…	…

Tabla 3.4-6 Ejemplo de criterio básico de impacto

Fuente: Los autores

3.4.2.5.4 Fuentes

Plan estratégico organizacional, requisitos legales, resultados de otros procesos de gestión de riesgos, información relevante de la organización.

3.4.2.6 Actividad 9: Definir el criterio básico de aceptación de riesgo

3.4.2.6.1 Detalle de actividad

El equipo de análisis realizará lo siguiente:

- Definir el criterio básico de aceptación del riesgo, indicando bajo qué condiciones el riesgo es aceptado, cada organización define su propia escala, se especifica en base a las políticas, metas, objetivos organizacionales e intereses de los interesados.
- Considerar que el criterio básico de aceptación del riesgo debe ser aprobado por la alta directiva y debe estar definido acorde a la metodología de

estimación del riesgo, criterio de evaluación del riesgo y criterio básico de impacto detallado en las actividades anteriores.

3.4.2.6.2 Resultados

Criterio básico de aceptación del riesgo. A continuación se muestra una plantilla de ayuda:

Resultados de definición del criterio básico de aceptación del riesgo		
Nivel de riesgo estimado	**Criterio de aceptación**	**Descripción**
Alto		
Medio		
Bajo		
Observaciones		
Fecha		
Realizado por		

Plantilla 3.4-9 Criterio básico de aceptación del riesgo

Fuente: Los autores

3.4.2.6.3 Recomendaciones

Se recomienda determinar el criterio de aceptación del riesgo, especificando claramente si se acepta o no se acepta el nivel de riesgo estimado. Adicionalmente se recomienda establecer una descripción narrativa de condiciones específicas de aceptación del riesgo. A continuación se detalla como referencia el siguiente esquema (con enfoque cualitativo):

Nivel de riesgo estimado	**Criterio de Aceptación**	**Descripción**
Alto	No se acepta	Los niveles de riesgo estimado alto, deben ser siempre tratados.
Medio	No se acepta	Los niveles de riesgo estimado medios deben ser analizados previo a definir el enfoque de tratamiento.
Bajo	Se acepta	Los niveles de riesgo estimado bajo, serán aceptados.

Tabla 3.4-7 Ejemplo de criterio básico de aceptación de riesgo

Fuente: Los autores

3.4.2.6.4 Fuentes

Plan estratégico organizacional.

3.4.2.7 Actividad 10: Definir la organización para la gestión de riesgos de seguridad de la información

3.4.2.7.1 Detalle de actividad

El equipo de análisis realizará lo siguiente:

- Definir los roles y responsabilidades de esta organización que incluye el desarrollo de procesos adecuados de la gestión de riesgos, la identificación y análisis de los interesados, la definición de roles y responsabilidades internas y externas, establecimiento de las relaciones entre la organización y los interesados, interfaces hacia los más altos niveles de funciones de gestión de riesgos, definición de caminos de escalamiento de decisión. Esta organización debe ser aprobada por la alta directiva.

3.4.2.7.2 Resultados

Definición de la organización para la gestión de riesgos de seguridad de la información. A continuación se muestra una plantilla de ayuda:

Resultados de definición de la organización para la gestión de riesgos de seguridad de la información		
Organización de seguridad de la información		
Nombre		
Integrantes		
Apellidos	Nombres	Cargo
Rol		
Responsabilidades		
Relaciones con la organización e interesados		
Interfaces hacia los altos niveles		
Caminos de escalamiento de decisión		
Observaciones		
Fecha		
Realizado por		

Plantilla 3.4-10 Definición de la organización de gestión de riesgos de seguridad de la información

Fuente: Los autores

3.4.2.7.3 Recomendaciones de implementación

Se recomienda que esta organización sea independiente del área de TIC, esta es la misma organización sobre la que se forma el núcleo del equipo de análisis.

3.4.2.7.4 Fuentes

Información relevante de la organización, para el efecto.

3.4.3 PROCESO DE IDENTIFICACIÓN DE RIESGOS

El proceso de identificación de riesgos en la organización, se realizará a partir de la identificación de los activos más importantes de acuerdo al alcance, se identificará las áreas de interés, requisitos de seguridad y controles existentes para cada activo. Luego, se identificará las amenazas a partir de las áreas de interés, tomando como ayuda los perfiles de amenaza genéricos, catálogo de amenazas y vulnerabilidades. Finalmente, en este proceso se realizará la identificación de vulnerabilidades tecnológicas a partir de la evaluación de los componentes de infraestructura seleccionados para el efecto.

3.4.3.1 Actividad 11: Identificar activos

3.4.3.1.1 Detalle de actividad

Los participantes, a través de talleres, realizarán lo siguiente:

- De acuerdo al contexto del alcance, y a través de talleres se identificará cuales son los activos que utilizan para ayudar a la organización en el cumplimiento de su misión y objetivos.
- Con la colaboración de miembros del equipo de análisis, se elegirá los activos más importantes (5 de forma referencial) con su respectiva justificación. Priorizándolos (tasándolos) de acuerdo a la consecuencia relacionada a la revelación, modificación, pérdida o interrupción de información. La consecuencia hace referencia a la pérdida de confidencialidad, disponibilidad e integridad.
- La escala de valor de los activos puede ser cuantitativa o cualitativa.

3.4.3.1.2 Resultados

Activos identificados. A continuación se muestra una plantilla de ayuda:

Resultados de identificación de activos					
Activo	**Razón de selección**	**Descripción acordada**	**Propietario**	**Categoría**	**Prioridad (tasación)**
Observaciones					
Fecha					
Realizado por					

Plantilla 3.4-11 Identificación de activos

Fuente: Los autores

3.4.3.1.3 Recomendaciones de implementación

Para facilitar la identificación de activos, se recomienda realizar una lluvia de ideas con los participantes, utilizando de forma referencial las siguientes categorías: sistemas, información, software, hardware y personas, instalaciones.

Posteriormente, para la elección de los activos más importantes (críticos), se requiere elegir los activos con la tasación más alta, para esto se requiere la participación de miembros del equipo de análisis, para el caso se recomienda la participación de una o dos personas del equipo, de acuerdo a trabajar con los participantes del taller en las actividades para el efecto.

Se recomienda utilizar una escala de valoración (tasación) cuantitativa con el objetivo de ordenar descendentemente a los activos de acuerdo a priorizarlos.

A continuación se muestra un esquema referencial de ejemplo:

Activo	**Razón de selección**	**Descripción acordada**	**Propietario**	**Categoría**	**Prioridad (Tasación)**
Sistema	El sistema A es	Sistema A	Departamen	Sistema	Utilizar una

A	indispensable para procesar la información de ventas de forma efectiva.	{esta descripción será la utilizada en adelante para referirse al activo}	to de ventas		escala numérica {1,2,3…}

Tabla 3.4-8 Ejemplo de matriz de identificación de activos

Fuente: Los autores

En base al cuadro anterior, los activos críticos serán aquellos 5 (cinco) activo con mayor tasación.

3.4.3.1.4 Fuentes

Información relevante para la organización para el efecto.

3.4.3.2 Actividad 12: Identificar las áreas de interés

3.4.3.2.1 Detalle de actividad

Los participantes a través de talleres, realizarán lo siguiente:

- Por cada activo se detectará escenarios que ponen en peligro a los activos sobre la base de las fuentes típicas de amenaza accidentales o deliberadas (actores humanos con acceso a red, actores humanos con acceso físico, problemas del sistema y otros problemas) y sus resultados (revelación, modificación, pérdida o interrupción de la información).
- Se determinará por cada escenario, el impacto (lo que pasaría si efectivamente este ocurre).

3.4.3.2.2 Resultados

Áreas de interés. A continuación se muestra una plantilla de ayuda:

Resultados de identificar las áreas de interés				
Activo 1				
Fuente de amenaza	**Nro.**	**Área de interés**	**Resultado**	**Impacto**
Acciones deliberadas o accidentales por personas	1			
	2			
	…			
Problemas de sistema	…			
	…			
	…			
Otros problemas	…			
	…			
Activo 2				
…	…			
Observaciones				
Fecha				
Realizado por				

Plantilla 3.4-12 Identificar áreas de interés

Fuente: Los autores

3.4.3.2.3 Recomendaciones de implementación

Para obtener la información acerca de las áreas de interés, se recomienda utilizar el siguiente esquema referencial por cada activo crítico:

Fuentes de amenaza		**Resultado**
Acciones deliberadas por personas (de dentro y fuera de la organización)		Revelación de información sensible.
Acciones accidentales por personas (de dentro y fuera de la organización o por uno mismo)		Modificación de información sensible.
Problemas de los sistemas (Defectos de hardware y/o software, inestabilidad de sistemas, código malicioso, otros)	**Activo**	Destrucción ó pérdida de hardware, software o información importante.
Otros problemas (perdidas de poder, indisponibilidad de agua, indisponibilidad de telecomunicaciones, desastres naturales, otros)		Interrupción de acceso a información, aplicaciones o servicios.

Tabla 3.4-9 Fuentes de amenaza vs Resultados

Fuente: Los autores

Posterior al realizar el análisis de acuerdo al esquema anterior, se podría obtener un área de interés como por ejemplo: “Personal accediendo a información en el Sistema

X (activo) que no está autorizado a utilizar, podría intencionalmente ingresar datos erróneos".

Área de Interés	**Resultado**	**Impacto**
Personal que accediendo al Sistema X (activo), podría intencionalmente ingresar datos erróneos.	Modificación {Modificación, Revelación, Pérdida, Interrupción}	Modificaciones incorrectas pueden afectar la productividad del personal.

Tabla 3.4-10 Ejemplo de áreas de interés vs resultados vs Impacto por activo

Fuente: Los autores

3.4.3.2.4 Fuentes

Información relevante para la organización, para el efecto.

3.4.3.3 Actividad 13: Identificar los requisitos de seguridad

3.4.3.3.1 Detalle de actividad

Los participantes, a través de talleres, realizarán lo siguiente:

- Se establecerá por cada activo, cada requisito (a través de una narración descriptiva) asociado a la confidencialidad, integridad y disponibilidad de la información.
- Se seleccionará el requisito más importante para cada activo.

3.4.3.3.2 Resultados

Requisitos de seguridad. A continuación se muestra una plantilla de ayuda:

Resultados de requisitos de seguridad			
Requisitos de seguridad			
Activo	**Confidencialidad**	**Integridad**	**Disponibilidad**
Observaciones			
{Por cada activo, el requisito de seguridad marcado con * es el más importante.}			
Fecha			
Realizado por			

Plantilla 3.4-13 Requisitos de seguridad

Fuente: Los autores

3.4.3.3.3 Recomendaciones de implementación

Con el objetivo de detallar los requisitos de seguridad por cada activo, se recomienda utilizar descripciones narrativas, por ejemplo, un requisito de disponibilidad para un Sistema X (activo), podría ser “La disponibilidad del sistema, requerida es 24x7”.

Por lo general, la confidencialidad no se aplica a los servicios como los relacionados a software comercial; tampoco aplica al hardware físico. Para el caso de las personas únicamente hay que centrarse en la disponibilidad.

Se puede utilizar de forma referencial, el esquema que a continuación se muestra:

Activo	**Requisitos de seguridad**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Sistema A	La confidencialidad debe cumplir con la norma A.	Únicamente usuarios autorizados pueden modificar la información.	* La disponibilidad del sistema, requerida es 24x7

Tabla 3.4-11 Ejemplo de requisitos de seguridad por activo

Fuente: Los autores

Se podría también marcar con un “*” el requisito de seguridad más importante por activo.

Considerar, que cada requisito de seguridad puede tener ninguna, una o más descripciones narrativas asociadas.

3.4.3.3.4 Fuentes

Información relevante para la organización, para el efecto.

3.4.3.4 Actividad 14: Identificar controles existentes.

3.4.3.4.1 Detalle de actividad

Los participantes, a través de talleres, realizarán lo siguiente:

- Evaluar las prácticas actuales de seguridad de la organización en contra del catálogo de prácticas asociado a la norma ISO/IEC 27002:2005, a través de encuestas.
- Registrar tanto lo que funciona como lo que no funciona para los 133 controles de la norma.
- Generar un resumen del cumplimiento de los controles en base a los dominios de la norma.

3.4.3.4.2 Resultados

Controles existentes. A continuación se muestra una plantilla de ayuda:

Resultados de definición de controles existentes				
Controles de la norma ISO/IEC 27002:2008				
Ítem	Sección	Control	Definición	Cumple si/no
A.5.1.1	Política de Seguridad	Documento de Política de Seguridad de la Información	La dirección debe aprobar y publicar un documento que contenga la política y comunicarlo a todos los empleados, según corresponda.	
A.5.1.2	Política de Seguridad	Revisión y Evaluación	La política se debe revisar regularmente con una planificación o por cambios significativos del negocio	
…	…	…	…	…
A.15.3.1	Consideraciones sobre auditoria de Sistemas	Controles de auditoria de sistemas	Las auditorías del sistema operativo se deben planificar y consensuar cuidadosamente a fin de minimizar el riesgo de interrupciones a los procesos de negocio.	
A.15.3.2	Consideraciones sobre auditoria de Sistemas	Protección de las herramientas de auditoria	El acceso a las herramientas de auditoria de sistemas se debe proteger para prevenir un posible uso indebido o comprometido.	
Observaciones				
Fecha				
Realizado por				

Plantilla 3.4-14 Definición de controles existentes

Fuente: Los autores

En el Anexo 6, se encuentra la plantilla completa para la definición de controles existentes.

3.4.3.4.3 Recomendaciones de implementación

Los resultados de las encuestas, deberían arrojar un resumen por ejemplo indicando que “No existe una política de seguridad de la información”. O en su defecto hacer referencia específica a que controles de los dominios de la norma se cumple, no se cumple o no aplica.

Realizar un taller por separado con el personal del área de tecnología para detectar los controles asociados a tecnología de la información. Se debe incluir en los talleres al área legal de la organización.

3.4.3.4.4 Fuentes

Norma ISO/IEC 27002:2005, documentación de controles, revisiones físicas en sitio y resultados de auditorías internas.

3.4.3.5 Actividad 15: Identificar amenazas

3.4.3.5.1 Detalle de actividad

El equipo de análisis realizará lo siguiente:

- Determinar a qué categorías de amenaza para perfil genérico de riesgo (actores humanos con acceso a red, actores humanos con acceso físico, problemas del sistema, otros problemas) se asocia el área de interés.
- Generar perfiles de amenaza realizando un mapeo en base al desglose de las áreas de interés en las propiedades de amenaza que son: activo, acceso, actor, motivo, resultado y adicionalmente las áreas de interés.
- Mapear las propiedades de amenaza en el árbol de amenaza basado en activos, considerando los cuatro árboles de amenaza genéricos que forman el perfil genérico de amenaza y que se basan en las categorías de amenaza (actores humanos con acceso a red, actores humanos con acceso físico, problemas del sistema, otros problemas), los árboles de amenaza genéricos se describen en el Anexo 4.
- Para la categoría de amenaza de “Otros problemas”, podrían haber actores que no fueron considerados en el perfil genérico de amenaza, estos deben ser incorporados al perfil de amenaza desarrollado.
- Definir el perfil genérico de amenazas para la organización en base al perfil genérico de amenazas. Para esto, se debe agregar los actores que no se encuentren definidos en el perfil genérico de riesgos relacionados que surgieron al desarrollar las áreas de interés mapeadas.
- Determinar amenazas adicionales de ser el caso, considerando las que deben ser agregadas al perfil de amenaza de acuerdo al catálogo de amenazas y vulnerabilidades proporcionado por la norma ISO/IEC 27005:2008.
- Revisar la consistencia de los perfiles de amenaza.

3.4.3.5.2 Resultados

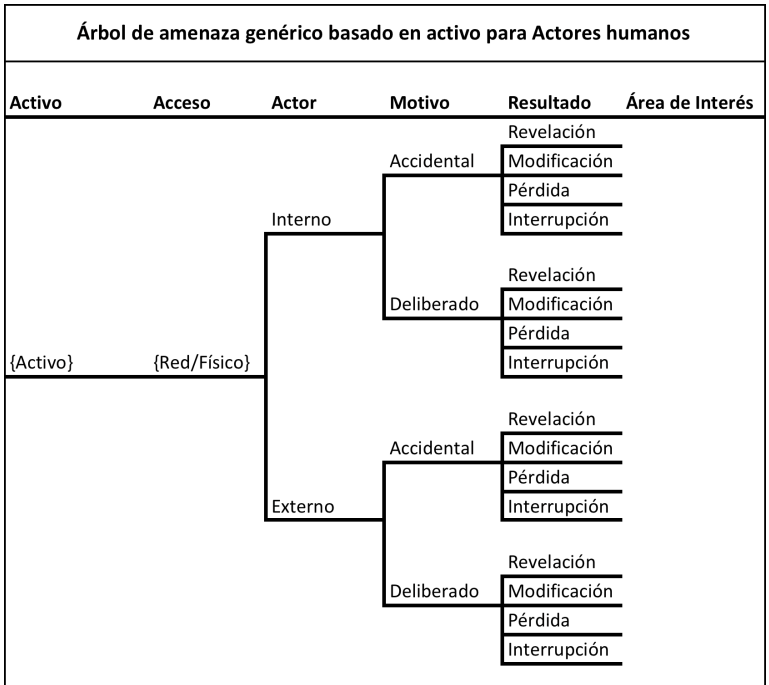
Perfiles de amenaza. A continuación se muestra las plantillas de ayuda para el mapeo a componentes de interés y los árboles de riesgo genéricos:

Resultado de identificar amenazas		
Activo: …. Mapeo de áreas de interés a propiedades de amenaza		
Área de Interés	**Activo**	
	Acceso	
	Actor	
	Motivo	
	Resultado	
…	…	…
Observaciones		
Fecha		
Realizado por		

Plantilla 3.4-15 Identificar Amenazas

Fuente: Los autores

Árbol de amenaza genérico basado en activo para Actores humanos



Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-16 Árbol de amenaza

Fuente: Los autores

En el Anexo 4, se puede observar los otros 3 árboles de amenaza genéricos.

3.4.3.5.3 Recomendaciones de implementación

Con el objetivo de generar los perfiles de amenaza, se recomienda trasladar las descripciones de las áreas de interés en las propiedades de los perfiles de amenaza, a continuación se muestra un esquema referencial de ejemplificación:

Área de interés	**Propiedades de amenaza**
1. Personal accediendo a información en el Sistema X, al cual no está autorizado usar	Activo: Sistema X Acceso: Red Actor: Interno Motivo: Accidental Resultado: Modificación

Tabla 3.4-12 Ejemplo de áreas de interés mapeadas a propiedades de amenaza

Fuente: Los autores

Los perfiles de amenaza se pueden representar de forma grafica, a continuación se muestra un esquema referencial de ejemplificación:

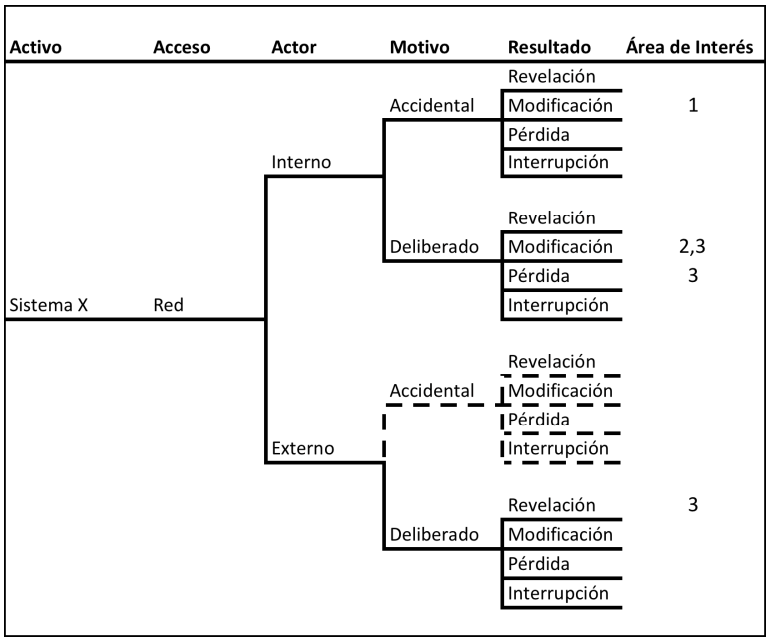


Figura 3.4-1 Ejemplo de árbol de amenaza con áreas de interés

Fuente: Los autores

Una vez generado el árbol de amenaza, se debe realizar un análisis de brechas determinando cuales de las ramas de línea punteada (las que indican que no hay riesgo), tienen posibilidad de que afecten al activo, para estos casos, se cambiará la línea punteada por línea continua, pero no se asocia a un área de interés. De esta forma, en el árbol de amenaza, se puede reconocer lo siguiente:

- Ramas de línea continua con área de interés: amenazas potenciales mapeadas de las áreas de interés.
- Ramas de línea continua sin áreas de interés: inicialmente no eran riesgo, sin embargo, luego del análisis de brechas, se determinó que si existía una posibilidad de amenaza al activo.
- Ramas de línea punteada, no representan riesgo.

Finalmente, se debe revisar la consistencia de los perfiles de amenaza, de acuerdo a los siguientes criterios:

- Relaciones entre los requerimientos de seguridad y los resultados, de acuerdo al siguiente esquema:

Requerimiento de seguridad	**Resultado**
Confidencialidad	Revelación
Integridad	Modificación
Disponibilidad	Pérdida, destrucción, interrupción

Tabla 3.4-13 Requerimientos de seguridad vs resultados

Fuente: Los autores

Para el caso, por ejemplo si se tiene la confidencialidad como requisito de seguridad de un activo, pero la revelación no aparece como salida, entonces hay que contemplar que la confidencialidad podría no ser un requerimiento de seguridad, que pudo haberse perdido amenazas que resulten en revelación, que no habría posibilidad de amenazas resultando en revelación de información ó que el requerimiento de seguridad podría ser guiado por una regulación antes que por una amenaza existente.

- Relaciones entre categorías de activos y perfiles de amenaza:

Tipo de Activo	Categoría de amenaza aplicables
Información electrónica	Los actores humanos con acceso a la red, los actores humanos con el acceso físico, los problemas de los sistemas, y otros problemas
Información física	Los actores humanos con el acceso físico y otros problemas
Sistemas en general, software y hardware	Los actores humanos con acceso a la red, los actores humanos con el acceso físico, los problemas de los sistemas, y otros problemas
Software (servicios)	Los actores humanos con acceso a la red, los actores humanos con el acceso físico, los problemas de los sistemas, y otros problemas
Hardware	Los actores humanos con el acceso físico y otros problemas.
Personas	Otros problemas

Tabla 3.4-14 Tipos de activo vs Categorías de amenaza aplicables

Fuente: Los autores

- Consistencia de los perfiles de amenaza entre los diferentes activos.

3.4.3.5.4 Fuentes

Áreas de interés, catálogo de amenazas y vulnerabilidades, norma ISO/IEC 27002:2005, revisión de incidentes, dueños de activos.

3.4.3.6 Actividad 16: Seleccionar los componentes de la infraestructura a evaluar

3.4.3.6.1 Detalle de actividad

En caso de optar por realizar esta actividad, el equipo de análisis con el apoyo de personal especializado de TI, realizará lo siguiente:

- Identificar el sistema de interés por cada activo (el más relacionado a este y es el que le da acceso al actor), a través de la revisión de los árboles de amenaza, enfocándose en los que están relacionados a actores humanos usando acceso a red.

- Identificar las clases de componentes clave (servidores, equipos de red, componentes de seguridad, estaciones de trabajo, computadores de hogar, portátiles, dispositivos de almacenamiento, dispositivos inalámbricos, etc.) asociados a componentes que son parte de un sistema de interés.
- Elegir los componentes de infraestructura a evaluar por cada clase de componente, la justificación y el enfoque (quien realizará la evaluación) y herramientas.

3.4.3.6.2 Resultados

Componentes de infraestructura a evaluar. A continuación se muestra una plantilla de ayuda:

Resultados de seleccionar los componentes de infraestructura a evaluar			
Activo	**Sistema de Interés**	**Clases de componentes clave**	**Razón de selección**
Observaciones			
Fecha			
Realizado por			

Plantilla 3.4-17 Clases de componentes de infraestructura a evaluar

Fuente: Los autores

Componentes de infraestructura a ser examinados				
Activo 1				
Clase de componente clave	**Dirección IP**	**Enfoque**	**Herramienta**	**Justificación**
Activo 2				
Clase de componente clave	**Dirección IP**	**Enfoque**	**Herramienta**	**Justificación**
Observaciones				
Fecha				
Realizado por				

Plantilla 3.4-18 Componentes de infraestructura a evaluar

Fuente: Los autores

3.4.3.6.3 Recomendaciones de implementación

Identificar los sistemas de interés (el más relacionado a este y es el que le da acceso al actor), a través de revisar los árboles de amenaza (enfocándose a actores humanos usando acceso a red) que conforman el perfil de amenaza, a través de examinar los posibles caminos de acceso de red, con la ayuda de la siguiente relación de las categorías de activos con los sistemas de interés:

Categoría de Activo	**Sistema de interés**
Activos de sistemas	Es el activo
Activos de información	Es el sistema más relacionado con la información
Activos de software	Es el sistema más relacionado con la aplicación o servicio.

Tabla 3.4-15 Categorías de activo vs Áreas de interés

Fuente: Los autores

Para un Sistema X (activo), el sistema de interés sería el mismo Sistema X.

Podría darse que se encuentre múltiples sistemas de interés para activos de información o software, pues estos por lo general se relacionan a múltiples sistemas, se debería considerar la posibilidad de dividir al activo en activos más pequeños.

Identificar las clases de componentes clave (servidores, equipos de red, componentes de seguridad, estaciones de trabajo, computadores de hogar, portátiles, dispositivos de almacenamiento, dispositivos inalámbricos, etc.) asociados a componentes que son parte de un sistema de interés, estableciendo la respectiva justificación, a continuación se muestra un esquema referencial al respecto que debe generarse por sistema de interés:

Clase de componente clave	**Razón para la selección**
Servidores	En estos servidores se almacena y procesa la información del sistema de ventas.
Equipo de red	…

Tabla 3.4-16 Ejemplo de razones de selección por clase de componente clave

Fuente: Los autores

Elegir los suficientes componentes de infraestructura a evaluar por cada clase de componente, para esto es necesario analizar la topología de la red, a continuación se muestra un esquema referencial al respecto que debe generarse por cada activo crítico:

Clase de componente clave	**Componente clave**	**Dirección IP/Nombre**	**Enfoque**	**Herramientas**	**Justificación**
Servidores	Equipo X	192,168.2.1 servidor1	Experto externo, Staff interno, Proveedor de servicios	Escáner de funcionamiento, de redes, híbridos, listas de verificación, scripts. (gratuitos, con costo)	La evaluación la realizará un experto externo debido a la falta de experiencia del personal interno al respecto.

Tabla 3.4-17 Ejemplo de lista de componentes de infraestructura a evaluar

Fuente: Los autores

En este tipo de evaluaciones es recomendable centrarse en las vulnerabilidades de configuración. Aún cuando existen vulnerabilidades de diseño e implementación.

Finamente, considerar las limitaciones, pues las herramientas de evaluación de vulnerabilidad no indican cuándo algunos de los procedimientos de administración del sistema están siendo utilizados indebidamente o se realizan incorrectamente.

3.4.3.6.4 Fuentes

Perfiles de amenaza, topología de red, herramientas de mapeo, listado de priorización de computadores.

3.4.3.7 Actividad 17: Identificar vulnerabilidades tecnológicas

3.4.3.7.1 Detalle de actividad

El equipo de análisis con el apoyo de personal especializado de TI y en base al enfoque de evaluación de vulnerabilidades, realizará lo siguiente:

- Ejecutar las herramientas de evaluación de la vulnerabilidad en los componentes de infraestructura ya seleccionados, considerando la información proporcionada por un catálogo de vulnerabilidades.
- Revisar las vulnerabilidades de tecnología detectadas con las herramientas, crear el resumen de resultados e interpretarlos.
- Refinar el resumen, generando las acciones y recomendaciones.
- Realizar un análisis de brechas entre los resultados de la evaluación y cada perfil de amenaza, revisando las ramas sin marcar del árbol de amenaza para los actores humanos con acceso a la red.
- Asociar las vulnerabilidades a los activos, los controles y amenazas.

3.4.3.7.2 Resultados

Listado de vulnerabilidades por activo. A continuación se muestra una plantilla de ayuda:

Resultados de Identificar vulnerabilidades					
Activo 1					
Clase de componente clave	**Dirección IP/Nombre**	**Herramienta**	**Se escaneó?**	**Resumen de vulnerabilidad (cantidad, tipo)**	**Recomendaciones**
Activo 2					
Clase de componente clave	**Dirección IP/Nombre**	**Herramienta**	**Se escaneó?**	**Resumen de vulnerabilidad (cantidad, tipo)**	**Recomendaciones**
Observaciones					
Fecha					
Realizado por					

Plantilla 3.4-19 Identificar vulnerabilidades

Fuente: Los autores

3.4.3.7.3 Recomendaciones de implementación

Posterior a ejecutar las herramientas de evaluación de la vulnerabilidad en los componentes de infraestructura seleccionados, es recomendable generar un reporte básico de ejecución, considerar el siguiente esquema referencial de acuerdo a llenar la plantilla propuesta en la sección anterior:

Componente de infraestructura	**Dirección IP/Nombre**	**Se escaneó (Si/No)**
Servidor transaccional	192.168.2.1 servidor2	Si

Tabla 3.4-18 Ejemplo de evaluación de vulnerabilidades tecnológicas

Fuente: Los autores

Las herramientas generan información como nombre de vulnerabilidad, descripción, nivel de severidad, y acciones para reparar.

Con los resultados de la evaluación, se puede crear un resumen de resultados, considerar el siguiente esquema referencial de acuerdo a llenar la plantilla propuesta:

Componente	**Dirección IP**	**Herramientas**	**Resumen de vulnerabilidad (cantidad, tipo)**
Servidor transaccional	192.168.2.1 servidor2	Script	1, alta 3, media 2, baja

Tabla 3.4-19 Ejemplo de resumen de resultados de evaluación de vulnerabilidades tecnológicas

Fuente: Los autores

Las acciones y recomendaciones generadas por las herramientas deben ser incluidas en un documento.

Finalmente, se debe realizar un análisis de brechas entre los resultados de la evaluación de vulnerabilidades y cada perfil de amenaza, revisando las ramas sin

marcar del árbol de amenaza para los actores humanos con acceso a la red, buscando posibles nuevas amenazas al activo crítico.

3.4.3.7.4 Fuentes

Componentes de infraestructura seleccionados, perfiles de amenaza, catálogo de vulnerabilidades, configuración de sistemas de información (HW, SW y comunicaciones).

3.4.4 PROCESO DE EVALUACIÓN DE RIESGOS

El proceso de evaluación de riesgos, realiza la identificación del impacto (consecuencia de un evento) a través de narraciones descriptivas para cada uno de los riesgos detectados en el proceso anterior, para la valoración del impacto será necesario comparar estas narraciones descriptivas con el criterio básico de impacto definido en el proceso de definición del contexto organizacional. De igual forma, para la valoración de la probabilidad, será necesario definir las descripciones de probabilidad para compararlas con el criterio de probabilidad que se define para este mismo proceso y es particular para cada riesgo y de la probabilidad de incidente. Posteriormente se debe aplicar la metodología de estimación del riesgo de acuerdo a obtener el nivel de estimación del riesgo.

3.4.4.1 Actividad 18: Identificar impacto

3.4.4.1.1 Detalle de actividad

Los participantes, a través de talleres realizarán lo siguiente:

- Identificar el impacto de las amenazas por resultado (revelación, modificación, pérdida, interrupción) a los activos críticos en relación a la misión organizacional, a través de descripciones narrativas de las repercusiones a la organización. Identificando las consecuencias que provocan perdida de confidencialidad, integridad y disponibilidad.
- Revisar los perfiles de amenaza, de acuerdo a encontrar los resultados (revelación, modificación, pérdida, interrupción) que aplican a ser revisados por cada activo.

- Asociar la consecuencia identificada a la sección correspondiente del perfil de amenaza (escenario de incidente).
- Utilizar cada una de las áreas de impacto como referencia para la identificación de las descripciones de impacto para activo crítico, relacionándolas a cada tipo de resultado.

3.4.4.1.2 Resultados

Impactos identificados. A continuación se muestra una plantilla de ayuda:

Resultado de identificar impacto	
Activo 1	
Resultado	**Descripción de Impacto**
Revelación	
Modificación	
Pérdida	
Interrupción	
Activo 2	
Resultado	**Descripción de Impacto**
Revelación	
Modificación	
Pérdida	
Interrupción	
...	
Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-20 Identificar Impacto

Fuente: Los autores

3.4.4.1.3 Recomendaciones de implementación

Con el objetivo de detallar el impacto de las amenazas por resultado, se recomienda revisar el siguiente ejemplo de descripciones de impacto:

Activo	**Resultado**	**Descripción de Impacto**
Sistema A	Revelación	Imagen: La revelación de información sensible puede provocar una pérdida de credibilidad por parte del cliente. Productividad: La revelación de información no afectaría la productividad. Multas y sanciones: La revelación de

		información sensible sería causa de multas por parte de los entes de control…
	Modificación	…
	Pérdida	…
	Interrupción	…

Tabla 3.4-20 Ejemplo de descripción de impacto por resultado y activo.

Fuente: Los autores

3.4.4.1.4 Fuentes

Áreas de interés, perfiles de amenaza, activos, amenazas, vulnerabilidades.

3.4.4.2 Actividad 19: Valorar el impacto de las amenazas

3.4.4.2.1 Detalle de actividad

Los participantes realizarán lo siguiente:

- Valorar el impacto, revisando las ramas de los árboles de los perfiles de amenaza, comparando el criterio básico de impacto con las descripciones de impacto por tipo de resultado (revelación, modificación, pérdida o interrupción) que se generaron en la actividad anterior. De acuerdo a eso, se elije uno de los valores de la escala definida en el criterio básico de impacto (por ejemplo: alto, medio o bajo).
- Agregar el valor de impacto al perfil de amenaza, creando así un perfil de riesgo

3.4.4.2.2 Resultados

Perfil de riesgo (perfil de amenaza con impacto valorado). A continuación se muestran las plantillas de ayuda:

Resultado de valorar impacto		
Activo 1		
Resultado	**Descripción de Impacto**	**Valor de Impacto**
Revelación		
Modificación		
Pérdida		
Interrupción		
Activo 2		
Resultado	**Descripción de Impacto**	**Valor de Impacto**
Revelación		
Modificación		
Pérdida		
Interrupción		
...		
Observaciones		
Fecha		
Realizado por		

Plantilla 3.4-21 Valorar impacto

Fuente: Los autores

Árbol de amenaza genérico basado en activo para Actores humanos						
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Área de Interés**	**Impacto**
{Activo}	{Red/Físico}	Interno	Accidental	Revelación		
				Modificación		
				Pérdida		
				Interrupción		
			Deliberado	Revelación		
				Modificación		
				Pérdida		
				Interrupción		
		Externo	Accidental	Revelación		
				Modificación		
				Pérdida		
				Interrupción		
			Deliberado	Revelación		
				Modificación		
				Pérdida		
				Interrupción		
Observaciones						
Fecha						
Realizado por						

Plantilla 3.4-22 Perfil de riesgo

Fuente: Los autores

El resto de perfiles de riesgo (árboles de amenaza con áreas de interés) con impacto valorado se pueden obtener a partir del resultado de la Actividad 15.

3.4.4.2.3 Recomendaciones de implementación

La asignación de los valores de impacto, se realiza en base a las descripciones de impacto generadas en la sección anterior, a continuación se muestra un ejemplo:

Activo	**Resultado**	**Descripción de Impacto**	**Valor de Impacto por área de impacto**	**Valor de Impacto consolidad**
Activo X	Revelación	Imagen: La revelación de información sensible puede provocar una pérdida de credibilidad por parte del cliente. Productividad: La revelación de información no afectaría la productividad. Multas y sanciones: La revelación de información sensible sería causa de multas por parte de los entes de control. ….	Medio (M) Bajo (B) Medio (M)	Medio a Bajo (M-B)
	Modificación	…	Alto (A)	Alto a Medio a

			Medio (M) Bajo (B) …	Bajo (A-M-B)
	Pérdida o destrucción	…	Alto (A) Alto (A) ..	Alto (A)
	Interrupción	…	Bajo (B) …	Bajo (B)

Tabla 3.4-21 Ejemplo de valoración de impacto por activo y resultado

Fuente: Los autores

Como se puede observar en el cuadro anterior las valoraciones de impacto pueden ser combinaciones entre Alto, Medio y Bajo, esto depende de la valoración que reciba cada área de impacto. Se recomienda utilizar los acrónimos A, M, y B, seguidos de un “guión”, indicando así los rangos. Para el caso de una valoración cuantitativa, este tipo de valoraciones puede ser definido en base a cálculos numéricos.

Por cada árbol de amenaza, se debe realizar el análisis de las descripciones de impacto por activo en relación al criterio básico de impacto y a las escalas definidas en la metodología de estimación de riesgo, se obtiene un perfil de amenaza con el impacto valorado, lo que forma un perfil de riesgo, que se puede apreciar en el siguiente esquema referencial a modo de ejemplo:

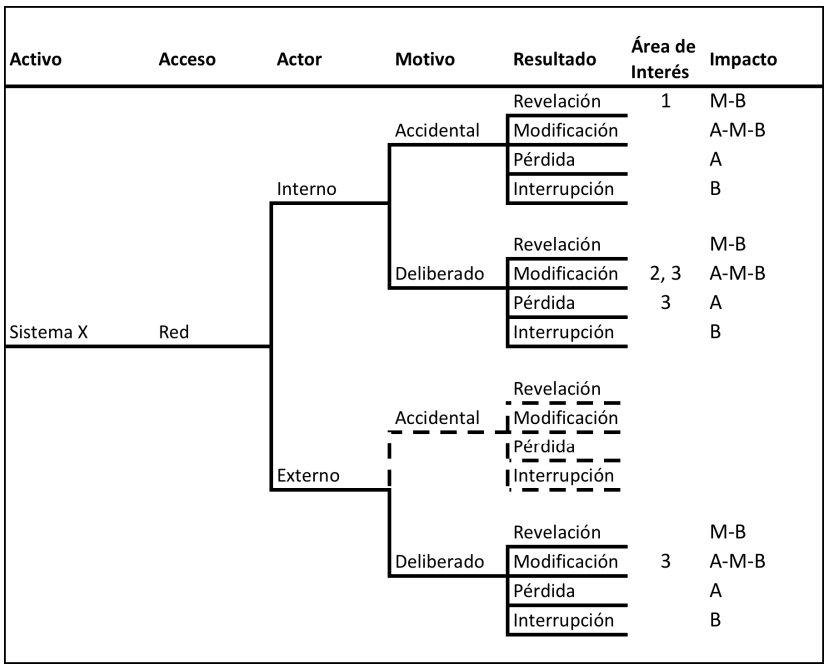


Figura 3.4-2 Ejemplo de perfil de riesgo

Fuente: Los autores

3.4.4.2.4 Fuentes

Perfiles de amenaza, descripción de impacto, criterio de evaluación de riesgo, criterio básico de impacto.

3.4.4.3 Actividad 20: Describir la probabilidad de amenazas

3.4.4.3.1 Detalle de actividad

Los participantes realizarán lo siguiente:

- Revisar en los perfiles de riesgo aquellos activos que son objetivos probables de amenaza por actores humanos, determinando los motivos, medios y oportunidad de amenaza humana con acceso de red o físico.
- Para todos los perfiles de riesgo, analizar datos históricos de ocurrencia para las amenazas y analizando circunstancias inusuales que afectarían la probabilidad de amenaza. Adicionalmente, buscar datos de cuan a menudo se dieron estos eventos en el pasado.

- Registrar la información obtenida como una narración descriptiva, el registro se realizará para todas las amenazas que apliquen en el perfil de riesgo.

3.4.4.3.2 Resultados

Descripción de probabilidad por cada amenaza. A continuación se muestra una plantilla de ayuda:

Resultado de describir probabilidad de amenaza					
Activo 1					
Acceso	Actor	Motivo	Resultado	Descripción de probabilidad	
				Motivos	
				Recursos	
				Oportunidad	
				Circunstancias inusuales de afectación	
				Referencias a datos históricos	
...					
Activo 2					
Acceso	Actor	Motivo		Descripción de probabilidad	
...					
Observaciones					
Fecha					
Realizado por					

Plantilla 3.4-23 Describir probabilidad de amenaza

Fuente: Los autores

3.4.4.3.3 Recomendaciones de implementación

Para la asignación de descripciones de probabilidad de impacto, recomienda revisar el siguiente esquema referencial de ejemplo:

Activo	Acceso	Actor	Motivo	Resultado	Descripción de probabilidad
Sistema A	Red	Interno	Accidental	Modificación	Motivos: Accidentalmente ingresar datos que el sistema no valida. Medios: Computador de oficina. Oportunidad: Al ingresar órdenes de compra. Referencia datos históricos: No se cuenta.

					Circunstancias inusuales: No se ha detectado.

Tabla 3.4-22 Ejemplo de asignación de descripciones de probabilidad de impacto

Fuente: Los autores

3.4.4.3.4 Fuentes

Planes organizacionales, requisitos legales, resultados de otros procesos de gestión de riesgos, referencias históricas de incidentes.

3.4.4.4 Actividad 21: Definir el criterio de probabilidad

3.4.4.4.1 Detalle de actividad

Los participantes realizarán lo siguiente:

- Definir lo que constituye una probabilidad de ocurrencia alta, media o baja (o su escala cuantitativa o cualitativa equivalente de acuerdo a la metodología de estimación de riesgo). Por ejemplo, una probabilidad de ocurrencia de 2 veces al año es media.
- Establecer un criterio de probabilidad único, analizando todas las descripciones de probabilidad establecidas en la actividad anterior. Se debe utilizar datos objetivos existentes en adición a la experiencia subjetiva.
- Considerar que esta tarea suele ser compleja debido a la falta de información histórica acerca de las ocurrencias de amenazas.

3.4.4.4.2 Resultados

Criterio de probabilidad. A continuación se muestra una plantilla de ayuda:

Resultado de definir criterio de probabilidad	
	Criterio de probabilidad
Alto	
Medio	
Bajo	
Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-24 Definir criterio de probabilidad

Fuente: Los autores

3.4.4.4.3 Recomendaciones de implementación

Se recomienda generar criterios de probabilidad individuales para cada amenaza, para posteriormente consolidarlas en un criterio único. Para esta actividad, se puede utilizar el siguiente esquema como referencia:

Resultado de definir criterio de probabilidad					
Activo 1					
Acceso	Actor	Motivo	Resultado	Criterio de probabilidad	
				Alto	
				Medio	
				Bajo	
...					
Activo 2					
Acceso	Actor	Motivo	Resultado	Criterio de probabilidad	
...					
Observaciones					
Fecha					
Realizado por					

Plantilla 3.4-25 Criterio de probabilidad individual

Fuente: Los autores

De acuerdo a establecer el criterio de probabilidad único, se recomienda revisar el siguiente ejemplo:

Alta	Media	Baja
Mayor a 12 veces al año	De una a 11 veces al año	Menos a una vez al año

Tabla 3.4-23 Ejemplo de criterio de probabilidad

Fuente: Los autores

3.4.4.4.4 Fuentes

Planes organizacionales, requisitos legales, resultados de otros procesos de gestión de riesgos, información relevante de la organización.

3.4.4.5 Actividad 22: Valorar la probabilidad de incidente

3.4.4.5.1 Detalle de actividad

Los participantes realizarán lo siguiente:

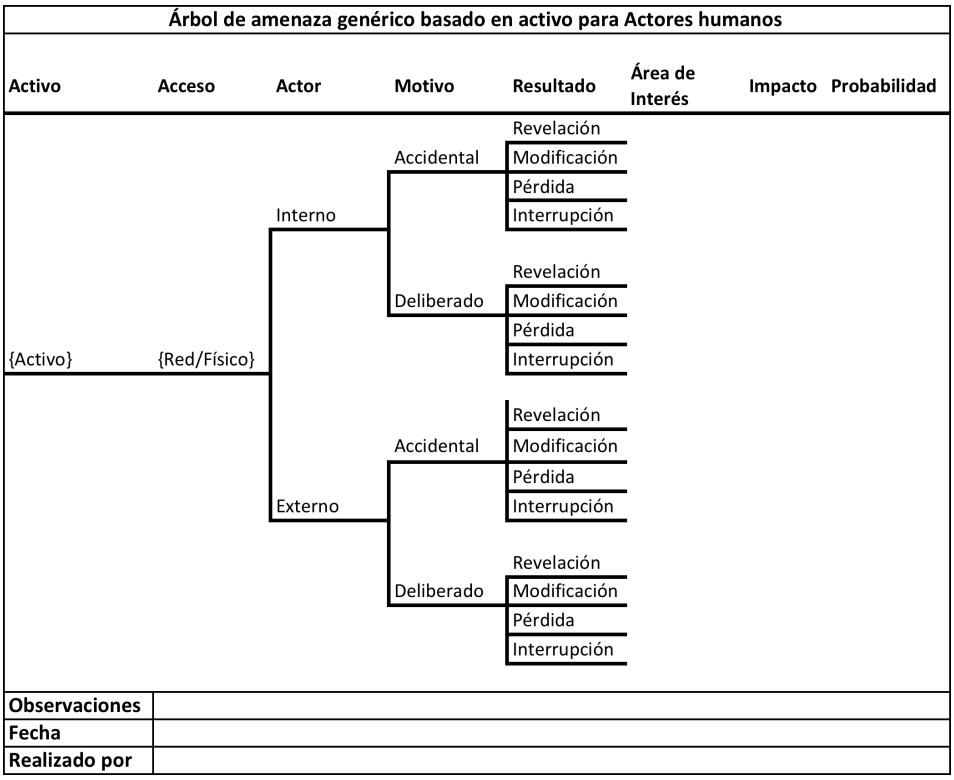
- Evaluar la probabilidad de las amenazas a los activos críticos y agregarla al perfil de riesgo, se realizará analizando las descripciones de probabilidad con

el criterio de probabilidad y ubicando el resultado de acuerdo a las escalas propuestas por la metodología de estimación del riesgo.

- Considerar adicionalmente la experiencia colectiva de los participantes.

3.4.4.5.2 Resultados

Perfiles de riesgo con probabilidad valorada. A continuación se muestra una plantilla de ayuda:



Plantilla 3.4-26 Perfil de riesgo con probabilidad e impacto

Fuente: Los autores

El resto de perfiles de riesgo (árboles de amenaza con áreas de interés) con impacto y probabilidad valorados se pueden obtener a partir del resultado de la Actividad 19.

3.4.4.5.3 Recomendaciones de implementación

Por cada árbol de amenaza, se debe realizar el análisis de las descripciones de probabilidad por activo en relación al criterio de probabilidad y a las escalas definidas en la metodología de estimación de riesgo, se obtiene un perfil de riesgo con

probabilidad valorada, se recomienda revisar en el siguiente esquema referencial de ejemplo:

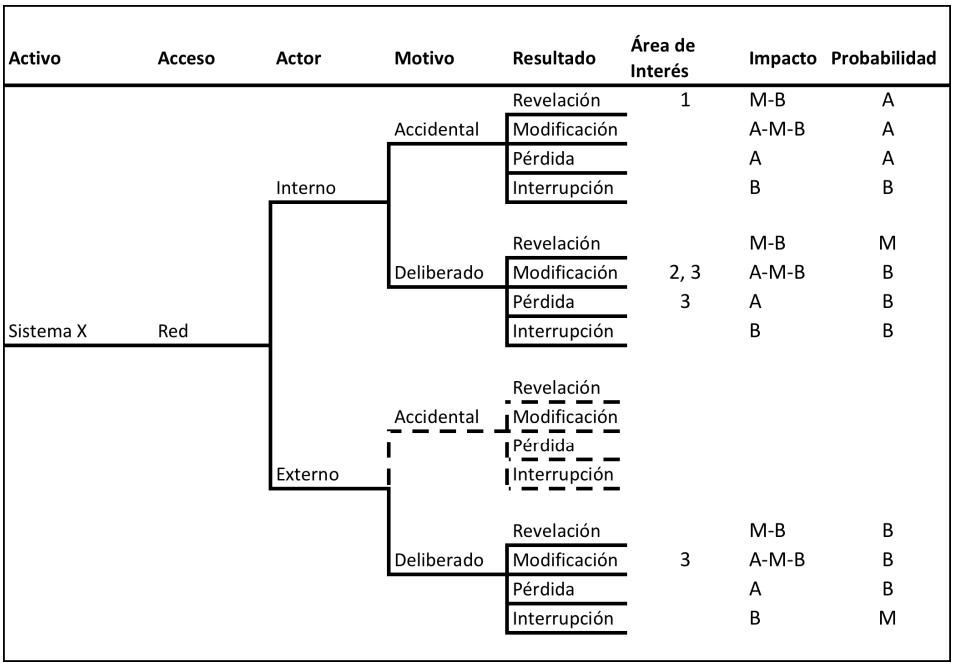


Figura 3.4-3 Ejemplo de perfil de riesgo con probabilidad e impacto valorados

Fuente: Los autores

3.4.4.5.4 Fuentes

Planes organizacionales, requisitos legales, resultados de otros procesos de gestión de riesgos, perfiles de riesgo, lista de controles existentes y planeados, su efectividad.

3.4.4.6 Actividad 23: Estimar (valorar) y priorizar el nivel de riesgo

3.4.4.6.1 Detalle de actividad

El equipo de análisis y personal de planificación estratégica, realizarán lo siguiente:

- Estimar el nivel de riesgo en base a aplicar la metodología de estimación de riesgo.
- Para el caso de utilizar el valor o pérdida esperada (producto del valor de impacto por la probabilidad en caso cuantitativo o de acuerdo por ejemplo a la matriz de valores esperados para caso cualitativo), se debe considerar

revisiones más profundas, pues se pondría el mismo esfuerzo para alta probabilidad y bajo impacto que para baja probabilidad y alto impacto (eventos catastróficos).

- Por cada amenaza en el perfil de riesgo, priorizar el riesgo estimado en base a analizarlo con el criterio de evaluación del riesgo.

3.4.4.6.2 Resultados

Nivel de estimación del riesgo, riesgos priorizados. A continuación se muestra una plantilla de ayuda:

Árbol de amenaza genérico basado en activo para Actores humanos

Activo	Acceso	Actor	Motivo	Resultado	Área de Interés	Impacto	Probabilidad	Riesgo Estimado	Prioridad
{Activo}	{Red/Físico}	Interno	Accidental	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
			Deliberado	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
		Externo	Accidental	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
			Deliberado	Revelación					
				Modificación					
				Pérdida					
				Interrupción					

Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-27 Perfil de riesgo con riesgo estimado y prioridad

Fuente: Los autores

El resto de perfiles de riesgo (árboles de amenaza con áreas de interés) con impacto, probabilidad se pueden obtener a partir del resultado de la Actividad 22.

3.4.4.6.3 Recomendaciones de implementación

Para el caso de un enfoque cualitativo, se podría considerar la matriz de valor esperado, que se muestra a continuación:

		Probabilidad		
		Alta	**Media**	**Baja**
I**mpacto**	**Alto**	Alto	Alto	Medio
	Medio	Alto	Medio	Bajo
	Bajo	Medio	Bajo	Bajo

Tabla 3.4-24 Matriz de valor esperado

Fuente: Método OCTAVE

Por cada árbol de amenaza, se debe obtener el valor esperado (riesgo estimado), de acuerdo a la metodología de estimación de riesgo, obteniendo un perfil de riesgo con valor esperado, que se puede apreciar en el siguiente esquema referencial:

Activo	Acceso	Actor	Motivo	Resultado	Área de Interés	Impacto	Probabilidad	Riesgo Estimado	Prioridad
Sistema X	Red	Interno	Accidental	Revelación	1	M-B	A	A-M	A,M,M
				Modificación		A-M-B	A	A-M	A,M,M
				Pérdida		A	A	A	A,M,M
				Interrupción		B	B	B	A,M,M
			Deliberado	Revelación		M-B	M	M-B	M,M,M
				Modificación	2, 3	A-M-B	B	M-B	M,M,M
				Pérdida	3	A	B	M	M,M,M
				Interrupción		B	B	B	M,M,M
		Externo	Accidental	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
			Deliberado	Revelación		M-B	B	B	M,M,B
				Modificación	3	A-M-B	B	M-B	M,M,B
				Pérdida		A	B	M	M,M,B
				Interrupción		B	M	B	M,M,B

Figura 3.4-4 Ejemplo de perfil de riesgo con estimación de riesgo y prioridad

Fuente: Los autores

En el esquema anterior se puede observar que los cruces entre probabilidad e impacto pueden resultar en estimaciones de riesgo basadas en rangos, por ejemplo M-B que quiere decir que es un riesgo estimado que va de medio a bajo. Para el efecto, al igual que en el caso de la valoración de impacto, se recomienda utilizar un guión "-" para separar los rangos de riesgo estimado.

La priorización del riesgo se obtiene a través de analizar los riesgos estimados con el criterio de evaluación de riesgo, este criterio puede tener varios enfoques, por ejemplo el valor estratégico de los procesos, los requerimientos legales y contractuales; los requerimientos y expectativas de los interesados. De acuerdo a esto, se recomienda describir los valores de priorización de riesgo utilizando los acrónimos A, M, y B separados por “comas”, indicando así la referencia cada criterio de evaluación de riesgo. Por ejemplo un valor de A, A, M podría reflejar un valor de riesgo alto para el primer y segundo criterio y medio para el último.

Es muy probable que en la primera aplicación del modelo sobre un proceso organizacional, se obtenga los mismos valores de priorización para todos los riesgos, esto debido a que todos los activos críticos pertenecen al mismo proceso, esto dado que el criterio de evaluación de riesgo es global para toda la organización. En este caso, es necesario orientar la prioridad para el tratamiento a los valores de riesgo estimado. Sin embargo, en siguientes iteraciones donde se tenga en cuenta riesgos asociados a diferentes procesos los valores asociados a la priorización de acuerdo al criterio de evaluación de riegos seguramente va a variar.

Finalmente, se recomienda generar un listado de todos los riesgos, ordenándolos de acuerdo a su prioridad, de mayor a menor, con el objetivo de contar con la lista de riesgos priorizados.

3.4.4.6.4 Fuentes

Norma ISO/IEC 27002:2005, prácticas actuales de seguridad, áreas de interés, perfiles de riesgo.

3.4.5 PROCESO DE TRATAMIENTO AL RIESGO

El proceso de tratamiento al riesgo se ejecuta si es que la evaluación de riegos ha generado la suficiente información para determinar el tratamiento al riesgo, caso contrario será necesaria otra iteración sobre la definición del contexto organizacional. De ser el caso, se define los lineamientos globales de protección a través de una estrategia de protección, posteriormente se establecerá los planes de mitigación en base al enfoque de riesgo (aceptar/mitigar). En caso de no llegar a un nivel de riesgo

aceptable, en base a la comparación del los resultados del tratamiento con el criterio de aceptación del riesgo generado en el proceso de definición del contexto organizacional, será necesaria otra iteración a la evaluación de riesgo. Caso contrario, se determinará la lista de acciones a corto plazo y sin mayor requerimiento de entrenamiento, que pueden aplicarse para tratar el riesgo. A partir de esto, se preparará una presentación para la alta directiva al respecto de los puntos clave de los riesgos y las soluciones propuestas. Finalmente se generará los siguientes pasos, es decir, información importante para aterrizar, apalancar e implementar la estrategia, plan y acciones.

3.4.5.1 Actividad 24: Crear una estrategia de protección

3.4.5.1.1 Detalle de actividad

El equipo de análisis y personal de planificación estratégica, realizarán lo siguiente:

- Desarrollar las estrategias de seguridad considerando los dominios de la norma ISO/IEC 27002:2005, que son acciones estratégicas de orientación a futuro tendiente a largo plazo, direccionadas a activar, iniciar, implementar y mantener su seguridad interna.
- Definir iniciativas estratégicas considerando cada dominio de los controles ISO/IEC 27002:2005, en base a responder las preguntas clave por cada una de estos dominios, estableciendo los enfoques acerca de las prácticas que se deben seguir utilizando, las que requieren mejorar y aquellas a adoptarse.

3.4.5.1.2 Resultados

Estrategia de protección. A continuación se muestra una plantilla de ayuda:

Resultados de definición de estrategia de protección			
Controles de la norma ISO/IEC 27002:2008			
Ítem	Sección	Preguntas Clave	Estrategias
A.5	Política de Seguridad		
A.6	Aspectos organizativos de seguridad de la información		
A.7	Gestión de activos		
A.8	Seguridad ligada a los recursos humanos		
A.9	Seguridad física y ambiental		
A.10	Gestión de comunicaciones y operaciones		
A.11	Control de accesos		
A.12	Adquisición, desarrollo y mantenimiento de sistemas de información		
A.13	Gestión de incidentes en la seguridad de la información		
A.14	Gestión de la continuidad del negocio		
A.15	Cumplimiento		
Observaciones			
Fecha			
Realizado por			

Plantilla 3.4-28 Definición de estrategia de protección

Fuente: Los autores

3.4.5.1.3 Recomendaciones de implementación

Para generar la estrategia de protección, se recomienda basarse en un esquema donde se separara los dominios de la norma ISO 27005, estableciendo un enfoque estratégico y respondiendo preguntas, de acuerdo a la siguiente referencia:

Dominio	Preguntas Clave	Enfoque estratégico
Control de accesos	Que se puede hacer para mejorar? Que se está haciendo mal? Prácticas actuales que se deben continuar utilizando? Nuevas estrategias a adoptar?	Enfoques de acuerdo a las respuestas de las preguntas.

Tabla 3.4-25 Ejemplo de enfoques estratégicos de tratamiento al riesgo

Fuente: Los autores

3.4.5.1.4 Fuentes

Norma ISO/IEC 27002:2005, prácticas actuales de seguridad (controles), áreas de interés, perfiles de riesgo.

3.4.5.2 Actividad 25: Crear planes de mitigación

3.4.5.2.1 Detalle de actividad

El equipo de análisis y personal de planificación estratégica, realizarán lo siguiente:

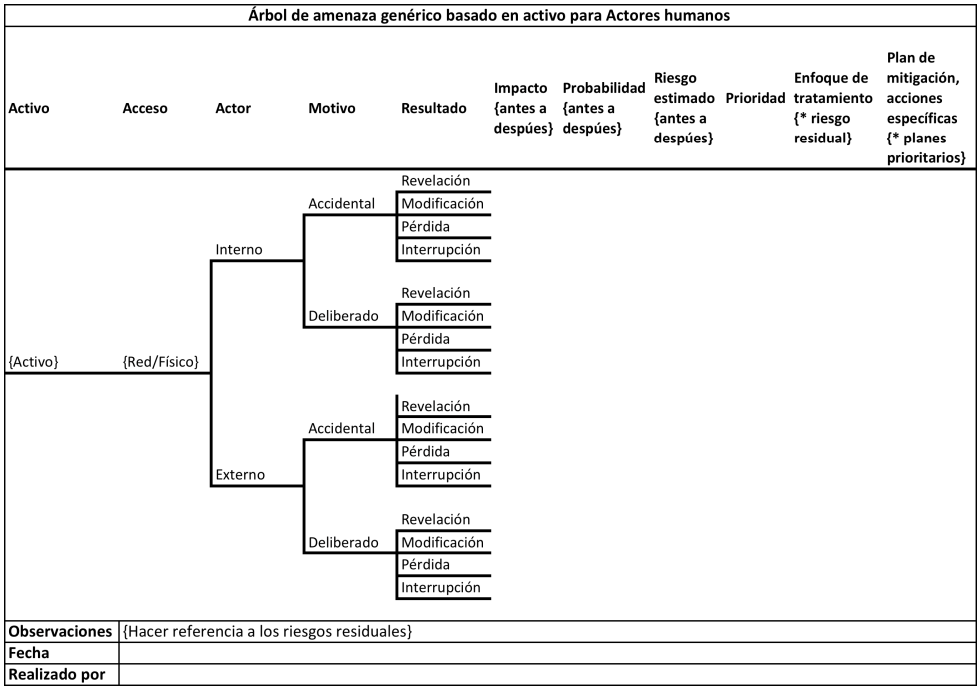
- Seleccionar el enfoque de mitigación por cada riesgo, se debe analizar las descripciones y valores de impacto, determinando la aceptación (retención), o mitigación (reducir, evitar, transferir ó una combinación) del riesgo, por lo general, se mitiga los riesgos con los valores de alto impacto, mientras que se acepta aquellos con valores de bajo impacto, esto debe ser determinado de acuerdo al criterio de aceptación de riesgo.
- Desarrollar planes de mitigación que son acciones operativas asociadas a las actividades necesarias para mitigar los riesgos y amenazas a los activos críticos, marcan la transición de la visión estratégica del riesgo a un enfoque más táctico u operativo, orientado a la reducción del impacto en la organización, pero más a menudo a reducir el riesgo de un activo crítico frente a la amenaza subyacente.
- Incluir en los planes, las acciones de mitigación que permitirían superar las amenazas a los activos críticos, considerando las prácticas que podrían implementarse para mitigar los riesgos.
- Considerar lo que se podría hacer para reconocer, resistir y recuperarse de las amenazas, adicionalmente se puede especificar medidas específicas para apoyar al éxito de los planes de mitigación.
- Considerar las restricciones de tiempo, financieras, técnicas, operacionales, culturales, étnicas, ambientales, legales, de facilidad de uso, personales que puedan afectar a los planes de mitigación.
- Revisar los planes de mitigación para buscar coherencia entre sí, y de haber alguna brecha, incorporarla en la estrategia de protección.

- Completar el perfil de riesgo con el enfoque y el plan de mitigación, estos deben ser consistentes de acuerdo a las alternativas de tratamiento:
    - Aceptación: Retener el riesgo sin ninguna acción adicional, en base a la evaluación del riesgo. No hay necesidad de implementar controles adicionales si el nivel del riesgo satisface el criterio de aceptación.
    - Mitigación: Reducir el riesgo a través de la selección de controles, de tal forma que el riesgo residual pueda ser re-valorizado hasta ser aceptable de acuerdo al criterio de aceptación. Se debe balancear el costo de implementación de controles con el valor de los activos protegidos.
    - Mitigación: Evitar el riesgo, si los riesgos son muy altos, con costos de implementación de tratamiento mayores a los beneficios, se puede evitar el riesgo mediante el retiro de una o varias actividades existentes o planificadas, o cambiando las condiciones sobre las cuales opera la actividad. Por ejemplo reubicar una localidad a otro sitio, a causa de un riesgo causado por la naturaleza.
    - Mitigación: Transferir los riesgos para que puedan ser gestionados más efectivamente, dependiendo de la evaluación del riesgo. Esta transferencia puede crear nuevos riesgos o modificar los existentes, por lo que se requiere tratamiento adicional. Puede ser posible transferir la responsabilidad de gestionar el riesgo, pero normalmente no es posible transferir la responsabilidad sobre el impacto.
- Apoyar los planes de mitigación con acciones específicas que apoyen al éxito del plan.
- Una vez definido el tratamiento del riesgo, se debe definir el riesgo residual, esto requiere una iteración sobre el proceso de evaluación del riesgo; es decir se definirá nuevamente el riesgo estimado tomando en cuenta los planes y acciones de tratamiento al riesgo. En caso de que el riesgo residual no sea aceptado, se requerirá una nueva iteración del tratamiento del riesgo.

- Definir la justificación para aquellos casos que no satisfagan el criterio de aceptación normal del riesgo que hayan sido aceptados.
- Se debe también priorizar los planes de mitigación en base a un análisis costo beneficio, ranking de riesgo estimado, considerando las acciones que mitigan riesgos asociados a más de un activo.
- Considerar que los riesgos raros, severos y de alto costo de implementación de tratamiento, comúnmente se integran al plan de continuidad de negocio organizacional.

3.4.5.2.2 Resultados

Perfiles de riesgo con planes de mitigación, riesgo residual y enfoque del tratamiento. A continuación se muestra una plantilla de ayuda:



Plantilla 3.4-29 Perfil de riesgo con planes de mitigación y acciones

Fuente: Los autores

El resto de perfiles de riesgo (árboles de amenaza con áreas de interés) con impacto, probabilidad y riesgo estimado se pueden obtener a partir del resultado de la Actividad 23.

3.4.5.2.3 Recomendaciones de implementación

Se recomienda cumplimentar los perfiles de riesgo con el enfoque y plan de mitigación específico, a continuación se muestra un ejemplo para el efecto:

Activo	Acceso	Actor	Motivo	Resultado	Impacto	Probabilidad	Riesgo Estimado	Prioridad	Enfoque de tratamiento	Plan de mitigación, acciones específicas
Sistema X	Red	Interno	Accidental	Revelación	M-B a B	A a M	A-M a B	A,M,M	Reducir	Lista de los planes, todos aplicarían para todas las ramas de este perfil de riesgo Se puede añadir medidas específicas de apoyo al éxito del plan.
				Modificación	A-M-B a M-B	A a M	A-M a M	A,M,M	*Reducir	
				Pérdida	A a M	A a M	A a M	A,M,M	*Reducir	
				Interrupción	B	B	B	A,M,M	Retener	
			Deliberado	Revelación	M-B a B	M a B	M-B a M	M,M,M	Reducir	
				Modificación	A-M-B a M-B	B	M-B a M	M,M,M	Reducir	
				Pérdida	A a M	B	M a B	M,M,M	Reducir	
				Interrupción	B	B	B	M,M,M	Retener	
		Externo	Accidental	Revelación						
				Modificación						
				Pérdida						
				Interrupción						
			Deliberado	Revelación	M-B a B	B	B	M,M,B	Retener	
				Modificación	A-M-B a M-B	B	M-B a B	M,M,B	Reducir	
				Pérdida	A a M	B	M a B	M,M,B	Reducir	
				Interrupción	B	M a B	B	M,M,B	Retener	
Observaciones	Los riesgos de actor interno con resultado de modificación o pérdida han generado un riesgo residual.									
Fecha										
Realizado por										

Figura 3.4-5 Ejemplo de perfil de riesgo con planes de mitigación y lista de acciones

Fuente: Los autores

En el perfil de riesgo anterior, se puede observar la transición que ha generado la iteración sobre la evaluación de riesgos sobre los valores de impacto, probabilidad y riesgo estimado. Adicionalmente, en los enfoques de riesgos se puede observar marcados con un "*" aquellos casos en que se generó un riesgo residual, es decir que el riesgo estimado no cumplió el criterio de aceptación del riesgo. Finalmente, en la sección de planes de mitigación se puede marcar con un "*" aquellos que tengan prioridad.

3.4.5.2.4 Fuentes

Prácticas actuales de seguridad (controles), norma ISO/IEC 27002:2005, áreas de preocupación, perfiles de riesgo, acciones recomendadas en base a vulnerabilidad, riesgo estimado y su priorización.

3.4.5.3 Actividad 26: Crear lista de acciones

3.4.5.3.1 Detalle de actividad

El equipo de análisis y personal de planificación estratégica, realizarán lo siguiente:

- Crear la lista de acciones, que la organización puede tomar en el corto plazo sin la necesidad de formación especializada, para superar las amenazas a los activos críticos; establecer un responsable, fecha de finalización y acciones de gestión requeridas.
- Considerar que esta lista de acciones se basa en las determinadas en la actividad anterior para apoyar al éxito de la implementación del plan.

3.4.5.3.2 Resultados

Lista de acciones. A continuación se muestra una plantilla de ayuda:

Resultado de crear lista de acciones			
Lista de acciones			
No.	Acción	Información	
		Responsable	
		Fecha de cumplimiento	
		Acciones de gestión requeridas	
...			
Observaciones			
Fecha			
Realizado por			

Plantilla 3.4-30 Crear acciones

Fuente: Los autores

3.4.5.3.3 Recomendaciones de implementación

Se recomienda revisar el siguiente ejemplo, de acuerdo a registrar el conjunto de lista de acciones:

Lista de acciones	
Ítem de acción	**Información**
Instalar software antivirus en los servidores	Responsabilidad: Administrador de servidores Fecha estimada: 01/01/2013 Acciones de gestión requeridas: Solicitar

	adquisición de licencias adicionales.

Tabla 3.4-26 Ejemplo de lista de acciones

Fuente: Los autores

3.4.5.3.4 Fuentes

Norma ISO/IEC 27002:2005, prácticas actuales de seguridad (controles), áreas de interés, perfiles de riesgo.

3.4.5.4 Actividad 27: Preparar la presentación de tratamiento al riesgo

3.4.5.4.1 Detalle de actividad

El equipo de análisis, realizará lo siguiente:

- Generar una presentación que incluya la información a fondo del riesgo y las soluciones propuestas.
- Considerar que esta presentación se la realizará a la alta directiva, con una revisión previa por parte del comité de seguridad, con el objetivo de que las soluciones planteadas sean aprobadas. Adicionalmente también debe ser aceptado el riesgo residual.

3.4.5.4.2 Resultados

Puntos clave de presentación de tratamiento al riesgo. A continuación se muestra una plantilla de ayuda:

Resultado de crear presentación de tratamiento del riesgo	
Puntos clave de la presentación	
Punto	**Descripción**
Información de activos.	
Prácticas de seguridad actuales.	
Riesgos identificados	
Estrategia de protección.	
Planes de mitigación.	
Listas de acciones.	
Riesgo residual.	
Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-31 Presentación de tratamiento del riesgo

Fuente: Los autores

3.4.5.4.3 Recomendaciones de implementación

Se recomienda incluir en cada punto clave de la presentación únicamente la información más relevante, de acuerdo al siguiente esquema:

Información de activos.- Incluir el nombre de cada activo crítico y una justificación concisa de la razón de su elección.

Prácticas de seguridad actuales.- Incluir el resumen por dominios de la norma ISO/IEC 27002:2005, se debe considerar tanto lo que se cumple como lo que no se cumple.

Riesgos identificados.- Incluir un resumen de los riesgos identificados, profundizando en los casos de los riesgos estimados como altos.

Estrategia de protección.- Incluir un resumen de la estrategia de protección, dividiéndolas por dominios de la norma ISO/IEC 27002:2005.

Planes de mitigación.- Incluir un detalle de los planes de mitigación, haciendo referencia explícita a aquellos planes que tienen mayor prioridad.

Listas de acciones.- Detallar la lista de acciones inmediatas incluyendo la fecha planificada para su cumplimiento.

Riesgo residual.- Detallar los riesgos residuales; es decir aquellos que no han cumplido con el criterio de aceptación del riesgo.

3.4.5.4.4 Fuentes

Estrategia de protección, planes de mitigación y lista de acciones

3.4.5.5 Actividad 28: Crear los siguientes pasos

3.4.5.5.1 Detalle de actividad

El equipo de análisis, realizará lo siguiente:

- Decidir en base a consultas a la alta directiva que acciones se van a tomar para dar apoyo a la puesta en práctica de la estrategia, planes de mitigación y lista de acción.

3.4.5.5.2 *Resultados*

Siguientes pasos. A continuación se muestra una plantilla de ayuda:

Resultado de crear los siguientes pasos	
Acciones de apoyo a la puesta en marcha del tratamiento al riesgo	
Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-32 Crear los siguientes pasos

Fuente: Los autores

3.4.5.5.3 Recomendaciones de implementación

Con el objetivo de establecer los siguientes pasos, se recomienda consultar a la alta directiva los siguientes lineamientos:

- Encontrar que se debe hacer para mejorar la seguridad de la información.
- Encontrar que se debe hacer para dar soporte a las iniciativas de mejora de seguridad.
- Definir la planificación para poner en marcha las posteriores actividades de mejora de seguridad.

3.4.5.5.4 Fuentes

Estrategia de protección, planes de mitigación y lista de acciones

3.4.6 PROCESO DE COMUNICACIÓN DEL RIESGO

El proceso de comunicación del riesgo, se enfoca en que el riesgo debe ser continuamente comunicado y entendido entre los entes de decisión y los interesados, a través de la organización para la gestión de riesgos de seguridad de la información.

3.4.6.1 Actividad 29: Comunicar el riesgo

3.4.6.1.1 Detalle de actividad

El comité de seguridad de la información en coordinación con el equipo de análisis, realizará lo siguiente:

- Compartir toda información obtenida en las fases de la gestión del riesgo como la existencia, naturaleza, forma, probabilidad, severidad, tratamiento y aceptación del riesgo con los interesados y otros entes de toma de decisiones, obteniendo así un continuo entendimiento del proceso de gestión de riesgos y sus resultados, de esta forma se puede alcanzar un acuerdo de cómo gestionar los riesgos.
- Ejecutar continuamente la comunicación del riesgo a través de planes, la coordinación entre quien toma decisiones y los interesados**.**

3.4.6.1.2 Resultados

Plan de comunicación del riesgo. A continuación se muestra una plantilla de ayuda:

Resultados de comunicación del riesgo	
Plan de comunicación del riesgo	
Objetivos	
A quien va dirigido	
Estrategias	
Observaciones	
Fecha	
Realizado por	

Plantilla 3.4-33 Plan de comunicación

Fuente: Los autores

3.4.6.1.3 Recomendaciones de implementación

Se recomienda mantener una comunicación bidireccional continua que logre acuerdos de cómo gestionar los riesgos mediante el intercambio de información entre los entes decidores y los interesados; a través de la coordinación del comité de seguridad de la información. Adicionalmente, es necesario desarrollar planes de comunicación para situaciones normales y de emergencia.

3.4.6.1.4 Fuentes

Toda información obtenida en las fases de gestión de riesgos de seguridad de la información.

3.4.7 PROCESO DE MONITOREO Y REVISIÓN DEL RIESGO

El proceso de monitoreo y revisión de riesgos se encarga de monitorear tanto los factores de riesgo así como la gestión de los riesgos, esto debido a que el riesgo y sus factores no son estáticos, permitiendo de esta forma mantener una imagen general del riesgo a través del tiempo, asegurando que los planes son los adecuados de acuerdo al contexto y que existen los recursos necesarios para llevarlos a cabo.

3.4.7.1 Actividad 30: Monitorear y revisar los factores de riesgo

3.4.7.1.1 Detalle de actividad

El comité de seguridad de la información en coordinación con el equipo de análisis, realizará lo siguiente:

- Generar un monitoreo y revisión continuo, para mantener la imagen general del riesgo, pues no son estáticos, sus factores varían en el tiempo, que incluye cambios de las amenazas, probabilidad, consecuencias, valor de los activos
- Incluir el monitoreo de nuevos activos del alcance, modificación del valor de los activos debido a cambios en los requerimientos del negocio, nuevas amenazas, nuevas o incrementadas vulnerabilidades, incremento del impacto de amenazas o vulnerabilidades valoradas, incidentes de seguridad.

3.4.7.1.2 Resultados

Plan de monitoreo y revisión. A continuación se muestra una plantilla de ayuda:

Resultados de monitorear y revisar factores de riesgo				
Reporte de monitoreo y revisión de factores de riesgo				
Nuevos activos incluidos en el alcance				
Activo	Fecha	Observaciones		
Cambios de requerimientos del negocio				
Cambio	Fecha	Observaciones		
Nuevas vulnerabilidades				
Vulnerabilidad	Fecha	Observaciones		
Incrementos de impacto o probabilidad de riesgos				
Riesgo	Variación de Impacto	Variación de probabilidad	Fecha	Observaciones
Incidentes de seguridad de la información				
Incidente	Activos afectados	Fecha	Observaciones	
Observaciones				
Fecha				
Realizado por				

Plantilla 3.4-34 Monitorear y revisar factores de riesgo

Fuente: Los autores

3.4.7.1.3 Recomendaciones de implementación

De forma general, se recomienda revisar los factores de riesgo cuando existen cambios mayores que puedan alterar el proceso de gestión de riesgos de seguridad de la información.

Se recomienda establecer reuniones periódicas entre los miembros de comité de seguridad de la información, de acuerdo a identificar los posibles cambios en los factores de riesgo de seguridad de la información.

3.4.7.1.4 Fuentes

Toda información obtenida en las fases de gestión de riesgos de seguridad de la información.

3.4.7.2 Actividad 31: Monitorear, revisar y mejorar de la gestión de riesgo

3.4.7.2.1 Detalle de actividad

El comité de seguridad de la información en coordinación con el equipo de análisis, realizará lo siguiente:

- Asegurar que el contexto, valoración, tratamiento, planes son apropiados para la circunstancia. Toda mejora sobre los procesos debe ser notificada a los respectivos administradores para asegurarse que el riesgo no está siendo desestimado o pasado por alto.
- Revisar los criterios de medición de riesgo para verificar que sean válidos de acuerdo a los objetivos del negocio y que estos cambios en el contexto son tomados en cuenta en los procesos de gestión del riesgo.
- Considerar el contexto legal y ambiental, de competencia, enfoque de evaluación, valor de activos y categorías, criterio de impacto, criterio de aceptación y evaluación, costo total de propiedad; y recursos necesarios.
- Asegurar que los recursos de valoración y tratamiento están disponibles para revisar los riesgos, crear o cambiar amenazas y vulnerabilidades. Adicionalmente, el monitoreo puede resultar en modificar o agregar el enfoque, metodología o herramientas usadas, dependiendo de los cambios identificados, iteraciones de valoración, objetivo y objetos del proceso de gestión de riesgos.

3.4.7.2.2 Resultados

Gestión del riesgo, monitoreada y revisada. A continuación se muestra una plantilla de ayuda:

Resultados de monitorear, revisar y mejorar la gestión de riesgos		
Reporte de monitoreo, revisión y mejora de la gestión de riesgos		
Contexto legal y ambiental		
Lineamiento	Fecha	Observación
Contexto de la competencia		
Lineamiento	Fecha	Observación
Enfoque de valoración de riesgo		
Lineamiento	Fecha	Observación
Importancia y categorías de activos		
Lineamiento	Fecha	Observación
Criterio de impacto		
Lineamiento	Fecha	Observación
Criterio de evaluación de riesgo		
Lineamiento	Fecha	Observación
Criterio de aceptación de riesgo		
Lineamiento	Fecha	Observación
Costo total de propiedad		
Lineamiento	Fecha	Observación
Recursos necesarios		
Lineamiento	Fecha	Observación
Observaciones		
Fecha		
Realizado por		

Plantilla 3.4-35 Monitorear, revisar y mejorar la gestión de riesgos

Fuente: Los autores

3.4.7.2.3 Recomendaciones de implementación

Se recomienda establecer reuniones periódicas entre los miembros del comité de riesgos de seguridad de la información, de acuerdo a identificar los posibles cambios en la gestión del riesgo de seguridad de la información.

3.4.7.2.4 Fuentes

Toda información obtenida en las fases de gestión de riesgos de seguridad de la información.

CAPÍTULO 4
APLICACIÓN AL CASO DE ESTUDIO

4.1 INTRODUCCIÓN

Con el objetivo de validar la aplicabilidad, afinar el modelo de gestión de riesgos de seguridad de la información propuesto, y conocer si efectivamente el modelo puede ser llevado a cabo como referencia en la gestión de riesgos de seguridad de la información de una organización, se aplicarán los procesos propuestos por dicho modelo al proceso de gestión de facturación de la Empresa Eléctrica Quito S.A a través de un caso de estudio establecido para el efecto.

4.2 PROCEDIMIENTO

El modelo de gestión de riesgos de seguridad de la información debe ser implementado sobre los procesos organizacionales de forma secuencial, se debe empezar por aquellos procesos que la organización considere más críticos.

Para efectos de la implementación se debe ejecutar cada proceso propuesto por el modelo, de forma secuencial. Sin embargo, el modelo podría requerir iteraciones sobre sus procesos debido a la naturaleza misma del riesgo y la complejidad de la gestión de riesgos de seguridad de la información, es decir está presente una naturaleza no lineal.

Una vez concluida la primera aplicación sobre un proceso, y al empezar la aplicación sobre el segundo proceso, será necesario realizar la siguiente iteración sobre el primer proceso, pues el contexto de riesgos es dinámico por tanto los cambios organizacionales podrían requerir aplicar los ajustes necesarios y de acuerdo a esto, el modelo debe aplicarse sobre la detección de estos cambios para ajustarse a las nuevas realidades para así ser efectivo en la gestión de riesgos de seguridad de la información.

Para el caso de estudio, se aplicará cada uno de los procesos del modelo de gestión de riesgos de seguridad propuesto al proceso de gestión de facturación de la

Empresa Eléctrica Quito S.A. La aplicación será secuencial y de acuerdo al orden establecido en el modelo, aún cuando podría requerirse iteraciones sobre los mismos procesos, debido a la las causas ya mencionadas. Sin embargo, hay que tener presente que los únicos procesos que no son secuenciales y son transversales a todo el modelo, son la comunicación y el monitoreo y revisión de riesgos, que se aplican de forma continua a través de todo el modelo.

4.3 APLICACIÓN A LA EMPRESA ELÉCTRICA QUITO S.A.

Se ha elegido a la Empresa Eléctrica Quito S.A, por ser la institución donde los autores forman la organización para la gestión de riesgos de seguridad de la información y cuentan con la apertura para aplicar el modelo de gestión de riesgos de seguridad de la información propuesto.

4.3.1 CARACTERIZACIÓN DE LA EMPRESA ELÉCTRICA QUITO

4.3.1.1 Reseña histórica

Iniciación del servicio

En el año 1895, por primera vez se instala en la ciudad de Quito la luz eléctrica. En los años 1895 y 1896, los señores Víctor Gangotena, Manuel Jijón y Julio Urrutia se asociaron para fundar una empresa que se denominó “La Eléctrica”.

Formación de la Empresa

La Empresa Eléctrica Municipal se convierte en una compañía autónoma, formada por acciones, con el nombre de Empresa Eléctrica Quito S.A. según consta en la escritura pública suscrita el 29 de septiembre de 1955 y teniendo como accionistas al Ilustre Municipio de Quito, a la Caja del Seguro y a la Caja de Pensiones, estas dos últimas fusionadas actualmente en una sola, denominada Instituto Ecuatoriano de Seguridad Social.

En el año 2009: Se suprime el Fondo de Solidaridad y su paquete accionario se transfiere, en representación del Estado, al Ministerio de Electricidad y Energía Renovable como accionista y tenedor del 56,992% del paquete accionario desde el 8

de diciembre de 2009, hasta el momento actual. La EEQ comienza a operar como Empresa Pública en virtud de la Disposición Transitoria Tercera del Mandato 15 y lo dispuesto en la Transitoria 2.2.1.5 de la Ley Orgánica de Empresas Publicas, publicada en el Registro Oficial No.48 del 10 de octubre de 2009.

4.3.1.2 Misión, Visión y Objetivos

Misión

Proveer a Quito y al área de concesión, el servicio público de electricidad de calidad, con eficiencia, solidaridad y responsabilidad socio ambiental, contribuyendo al desarrollo del sector eléctrico y la construcción del buen vivir.

Visión

Ser referente en el contexto nacional y regional, por la calidad y eficiencia en la prestación del servicio público de electricidad y por su aporte al desarrollo sostenible de la comunidad.

Objetivos

- Incrementar la satisfacción de los consumidores en la calidad del producto y servicio.
- Incrementar la población con servicio.
- Incrementar el uso eficiente de los recursos.
- Incrementar la eficiencia energética.
- Incrementar el uso de fuentes de energía alternativas.
- Incrementar la satisfacción de los Grupos de Actores con una gestión socialmente responsable.
- Incrementar la eficiencia institucional.
- Incrementar el uso de tecnología de punta que optimice la gestión.
- Incrementar el desarrollo del talento humano.

4.3.1.3 Mapa de procesos

A continuación se muestra el mapa de procesos de la Empresa Eléctrica Quito S.A.

Figura 4.3-1 Mapa de procesos EEQ

Fuente: Plan estratégico EEQ

De acuerdo al mapa de procesos ilustrado en la sección anterior se puede observar que el proceso correspondiente a la Gestión de tecnología de información y comunicaciones es un proceso de soporte a los procesos de la cadena de valor. Adicionalmente, se puede observar que el proceso de gestión de facturación forma parte de la cadena de valor organizacional.

4.3.1.4 Unidad de TI y posición en la toma de decisiones

La unidad de TI de la Empresa Eléctrica Quito, es la Dirección de tecnología de información y comunicaciones. En la estructura orgánica, la Dirección de tecnología de información y comunicaciones está ubicada bajo la Gerencia de Planificación, por tanto no está directamente bajo la Gerencia General.

A continuación se muestra la gráfica del orgánico funcional de la Empresa Eléctrica Quito:

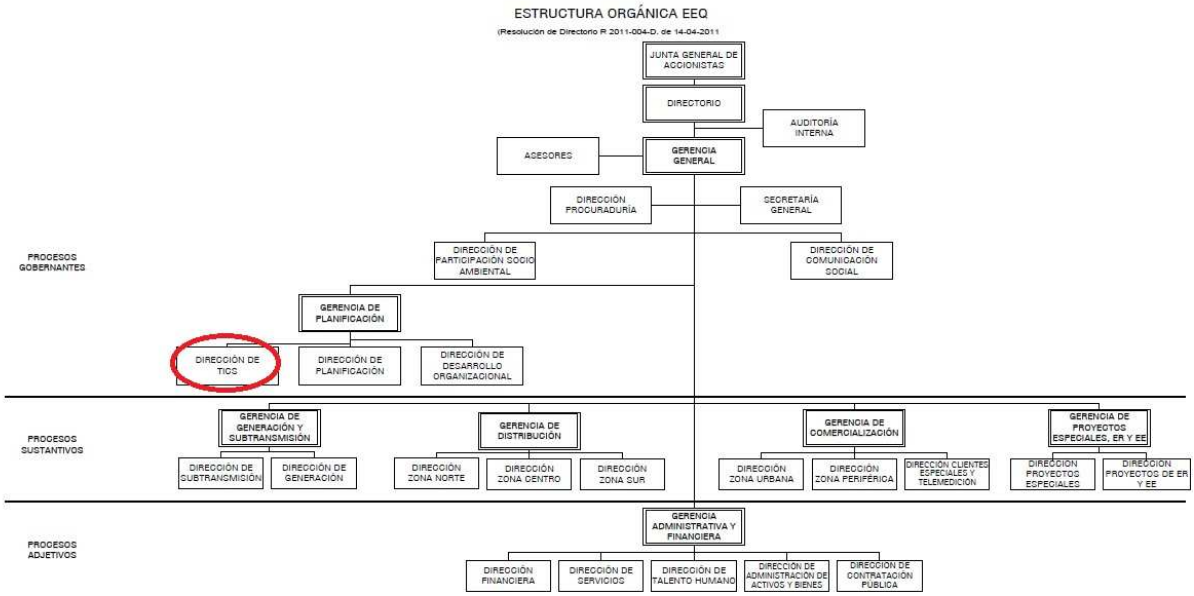


Figura 4.3-2 Estructura Orgánica de la Empresa Eléctrica Quito

Fuente: Plan estratégico EEQ

4.3.1.5 Organización para la gestión de riesgos de seguridad de la información y su posición

La organización para la gestión de riesgos de seguridad de la información, actualmente está bajo la Dirección de tecnología de información y comunicaciones, es decir no es un ente independiente a la gestión de tecnología de información y comunicaciones.

A continuación se muestra el orgánico estructural de la Dirección de tecnología de información y comunicaciones:

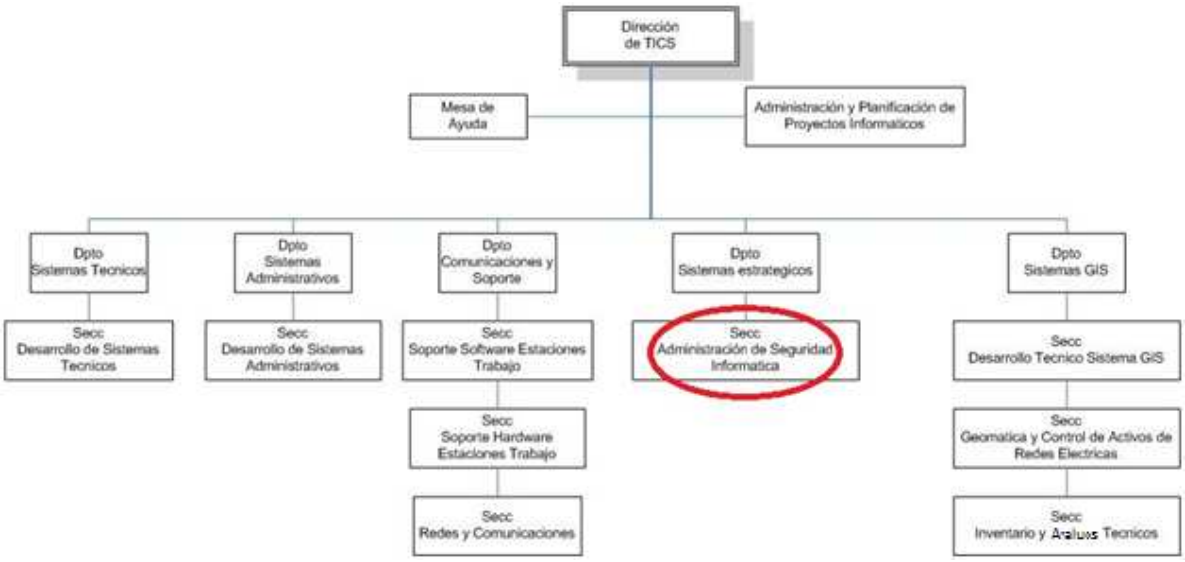


Figura 4.3-3 Orgánico estructural de la Dirección de tecnología de información y comunicaciones

Fuente: Plan estratégico Dirección de TIC EEQ

4.3.2 APLICACIÓN DEL MODELO

Con el objetivo de aplicar el modelo de gestión de seguridad de la información propuesto, a continuación se detalla la descripción de la ejecución de los procesos a nivel de actividades, indicando a detalle cómo se realizó el proceso, los resultados que se obtuvieron, las observaciones encontradas y las recomendaciones.

Se utilizará el acrónimo de EEQ para referirse a la Empresa Eléctrica Quito S.A.

4.3.2.1 Proceso de Iniciación

4.3.2.1.1 Actividad 1: Preparación

4.3.2.1.1.1 Detalle de ejecución

El jefe de la organización para la gestión de riesgos de seguridad de la información de la organización se auto-nombró el coordinador, de acuerdo a propiciar el surgimiento de la iniciativa de ejecutar acciones enfocadas a la gestión de riesgos de seguridad de la información. El coordinador gestionó la incorporación de una persona adicional de la organización para la gestión de riesgos de seguridad, con el objetivo de que le apoye en aspectos relacionados con la logística, documentación de las

actividades posteriores. Finalmente el coordinador estableció en cronograma de actividades asociado a la implementación del modelo.

4.3.2.1.1.2 Resultado obtenido

Resultados de actividades de preparación	
Definición de personal	
Coordinador de implementación	
Apellido	Carrera
Nombre	Walter
Cargo	Jefe de Sección de Seguridad de la Información
Unidad Organizacional	Sección de Seguridad de la Información
Personal de logística	
Apellido	García
Nombre	Santiago
Cargo	Ingeniero en Sistemas
Unidad Organizacional	Sección de Seguridad de la Información
Personal de documentación	
Apellido	García
Nombre	Santiago
Cargo	Ingeniero en Sistemas
Unidad Organizacional	Sección de Seguridad de la Información
Observaciones	
Fecha	18-jun-12
Realizado por	Walter Carrera

Resultado 4.3-1 Actividades de preparación

Fuente: Los autores

Cronograma de actividades																									
Semanas	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
Iniciación																									
1. Actividades de preparación	X																								
2. Obtener el patrocinio de la alta dirección		X																							
3. Seleccionar los miembros del equipo de análisis		X																							
Contexto Organizacional																									
4. Definir el alcance			X																						
5. Selección de los participantes			X																						
6. Determinar la metodología de estimación de riesgo				X																					
7. Definir el criterio básico de evaluación de riesgo					X	X																			
8. Definir el criterio básico de impacto					X	X																			
9. Definir el criterio básico de aceptación de riesgo					X	X																			
10. Definir la organización para la gestión de riesgos de seguridad de la información							X																		
Identificación de riesgos																									
11. Identificar activos								X																	
12. Identificar las áreas de interés									X	X															
13. Identificar requisitos de seguridad									X	X															
14. Identificar controles existentes											X														
15. Identificar amenazas												X													
16. Identificar componentes de infraestructura a evaluar													X												
17. Identificar vulnerabilidades														X											
Evaluación de riesgos																									
18. Identificar impacto (consecuencias)															X										
19. Valorar el impacto de las amenazas																X									
20. Describir la probabilidad de incidente																	X	X							
21. Definir el criterio de probabilidad																			X						
22. Valorar la probabilidad de incidente																			X						
23. Estimar (valorar) y priorizar el nivel de riesgo																				X					
Tratamiento al riesgo																									
24. Crear una estrategia de protección																					X	X			
25. Crear planes de mitigación																							X	X	
26. Crear lista de acciones																									X
27. Preparar la reunión con la alta dirección																									X
28. Crear los siguientes pasos																									X

Resultado 4.3-2 Diagrama Gantt (cronograma)

Fuente: Los autores

4.3.2.1.1.3 Observaciones

Se observó que el coordinador conocía el modelo de gestión de riesgos propuesto dado que lo desarrolló, además era conocedor del método OCTAVE y la norma ISO/IEC 27005:2008, asunto que propició que el modelo de gestión de riesgos propuesto fuese de su total conocimiento y no requiera capacitación adicional al respecto.

4.3.2.1.1.4 Recomendaciones

En la mayoría de casos en lo que se quiera implementar el modelo de gestión de riesgos de seguridad propuesto, el coordinador no tendrá conocimiento respecto al modelo, será necesario que este se auto capacite al respecto.

4.3.2.1.2 Actividad 2: Obtener patrocinio de la alta dirección

4.3.2.1.2.1 Detalle de ejecución

El coordinador ha planificado una reunión con los gerentes de la EEQ, a través de una invitación realizada por el gerente asociado a la Dirección de tecnología de información y comunicaciones. De acuerdo a esto, en primera instancia el coordinador solicitó el apoyo de la jefatura de la Dirección de tecnología de información y comunicaciones, para obtener este apoyo, previamente socializó el modelo a la mencionada jefatura.

La reunión se llevó a cabo realizando una explicación clara y concisa acerca de los objetivos de gestión de riesgos de seguridad de la información, y de la importancia de la activa participación de las gerencias en la implementación del modelo propuesto. De acuerdo a esto, la alta directiva aprobó el patrocinio del proyecto.

Adicionalmente, se definió la lista de personas que conformarán el comité de seguridad de la información, donde se incluyó a representantes de la Dirección de talento humanos, de la Dirección de tecnología de información y comunicaciones, de la organización para la gestión de riesgos de seguridad de la información y de procuraduría (área legal). Se cumplimentó esta definición determinando la misión de

este comité, que consiste en coordinar la comunicación acerca de riesgos de seguridad de la información entre los interesados y quienes toman las decisiones en la Empresa Eléctrica Quito. Este comité también debatirá acerca del riesgo, su priorización, aceptación, y tratamiento. Sin embargo no aprobará ningún criterio ni enfoques de tratamiento, pues únicamente realizará revisiones al respecto.

4.3.2.1.2.2 Resultado obtenido

Resultado de patrocinio de la alta dirección		
Asistentes a la reunión		
Apellido	**Nombre**	**Cargo**
		Gerente General
		Gerente de Comercialización
		Gerente Administrativo
		Gerente de Planificación
		Gerente de Distribución
		Gerente de Generación
		Procurador
		Director de TIC
Carrera	Walter	Jefe de sección de Seguridad de la información
García	Santiago	Ingeniero en sistemas
Puntos tratados y acuerdos		
Presentación del modelo de gestión de riesgos de seguridad de la información. Aprobación de la alta dirección al proyecto. Definición del alcance asociado al proceso de Gestión de facturación. El comité de seguridad de la información estará conformado por el Director de talento humano, Procurador, Director de tecnología de la información y comunicaciones, Jefe de la sección de seguridad de la información ó sus delegados.		
Observaciones		
Fecha	25-jun-12	
Realizado por:	Carrera Walter	
	García Santiago	

Resultado 4.3-3 Patrocinio de la alta dirección

Fuente: Los autores

4.3.2.1.2.3 Observaciones

Adicionalmente, en la menciona reunión, se trató de forma inicial el tema del alcance de la implementación, teniendo como acuerdo común de las gerencias, empezar por el proceso de facturación que es parte de la cadena de valor.

4.3.2.1.2.4 Recomendaciones

En la reunión se observó que fue necesario realizar una pequeña inducción inicial acerca de los riesgos de seguridad de la información, enmarcados en un marco

conceptual conciso. Con la ayuda de esta inducción, se facilitó el entendimiento del propósito que tiene el modelo de gestión de riesgos de seguridad de la información.

4.3.2.1.3 Actividad 3: Seleccionar a los miembros del equipo de análisis

4.3.2.1.3.1 Detalle de ejecución

El coordinador ha designado los miembros del equipo de análisis incluyéndose en el mismo, también ha incluido a una persona más de la organización para la gestión de riesgos de seguridad de la información de EEQ. Adicionalmente ha incluido en el equipo a una persona determinada por el área de negocio relacionada al proceso de facturación y a una persona de la Dirección de tecnología de información y comunicaciones.

4.3.2.1.3.2 Resultado obtenido

Equipo de análisis conformado.

Resultado de selección de miembros del equipo de análisis			
Equipo de análisis			
Apellido	**Nombre**	**Cargo**	**Unidad Organizacional**
Carrera	Walter	Jefe de Sección de Seguridad de la Información	Sección de Seguridad de la Información
García	Santiago	Ingeniero en Sistemas	Sección de Seguridad de la Información
		Ingeniero en Sistemas	Dirección de Tecnología de información y comunicaciones
		Gerente de Comercialización	Gerencia de Comercialización
Observaciones	La Gerencia de Comercialización podrá delegar a otro funcionario a ejecutar las tareas del equipo de análisis en razón de la disponibilidad de su tiempo		
Fecha	28-jun-12		
Realizado por	Carrera Walter		
	García Santiago		

Resultado 4.3-4 Selección de miembros del equipo de análisis

Fuente: Los autores

4.3.2.1.3.3 Observaciones

Se planificó y llevó una capacitación-taller para el equipo de análisis respecto al modelo de gestión de riesgos de seguridad de la información.

4.3.2.1.3.4 Recomendaciones

Se recomienda que la organización para la gestión de riesgos de seguridad de la información no dependa de la Dirección de tecnología de la información y comunicaciones, esto de acuerdo a evitar ser juez y parte en los procesos.

4.3.2.2 Proceso de definición del contexto organizacional

4.3.2.2.1 Actividad 4: Definir el alcance

4.3.2.2.1.1 Detalle de ejecución

En la actividad de obtención del patrocino de la alta dirección, se había ya llegado a un acuerdo acerca del alcance de la implementación. Por tanto en esta actividad no fue necesario establecer otra reunión al respecto. Dado que el alcance ya fue definido por la alta directiva, únicamente fue necesario que el equipo de análisis determine a detalle las áreas de la organización que participarían en la implementación. Estas áreas corresponden al proceso de facturación.

4.3.2.2.1.2 Resultado obtenido

Resultados de definición de alcance	
Detalle de alcance	
Macro proceso	Comercialización
Proceso	Facturación
Áreas involucradas	Dirección de TIC
	Facturación
	Rural
Observaciones	
La definición del alcance se había determinado ya en la obtención de la aprobación de la alta dirección. Por tanto fue necesario únicamente detallar las áreas operativas implicadas.	
Fecha	02-jul-12
Realizado por	El equipo de análisis

Resultado 4.3-5 Definición del alcance

Fuente: Los autores

4.3.2.2.1.3 Observaciones

No fue posible establecer formalmente el alcance en un acta, de acuerdo a lo que indica la guía de implementación, debido a la poca disponibilidad de tiempo de la alta directiva, sin embargo se considera suficiente el auspicio logrado.

4.3.2.2.1.4 Recomendaciones

Dado que es generalmente difícil contar con mucho tiempo para las reuniones con a alta directiva, es recomendable considerar incluir la definición del alcance en una sola actividad consolidada con la obtención del auspicio de la alta directiva.

4.3.2.2.2 Actividad 5: Selección de los participantes

4.3.2.2.2.1 Detalle de ejecución

El equipo de análisis ha determinado la lista de participantes tomando como referencia la mayor experiencia y conocimiento de los procesos, para esto fue necesario consultar la alta directiva quien realizó las respectivas gestiones para llegar a una determinación. Adicionalmente se definió quien sería la persona de respaldo, es decir aquella que participaría en caso de que el participante principal no pueda asistir a un determinado taller.

Se conformó la lista de participantes con 6 personas entre principales y respaldos. Los participantes fueron capacitados a través de varios talleres en el modelo de gestión de riesgos de seguridad.

4.3.2.2.2.2 Resultado obtenido

Resultados de selección de participantes			
Detalle de participantes			
Apellido	**Nombres**	**Área operativa**	**Tipo (Principal/Alterno)**
		Normalización	Principal
		Normalización	Alterno
		Rural	Principal
		Rural	Alterno
		Dirección de TIC	Principal
		Dirección de TIC	Alterno
Observaciones			
Fecha	12-jul-12		
Realizado por	El equipo de análisis		

Resultado 4.3-6 Selección de participantes

Fuente: Los autores

4.3.2.2.2.3 Observaciones

No fue posible formalizar la definición de los participantes en un acta, sin embargo esto quedó registrado a través de correos electrónicos.

4.3.2.2.2.4 Recomendaciones

Es recomendable formalizar de alguna manera el comprometimiento de los participantes a partir de los talleres, para el caso es necesario, contar al menos con un correo electrónico donde el alto directivo asociado al proceso de facturación comprometa a los participantes a participar activamente en los talleres.

4.3.2.2.3 Actividad 6: Determinar la metodología de estimación de riesgo

4.3.2.2.3.1 Detalle de ejecución

El equipo de análisis, en base a la guía de implementación, ha determinado que la metodología de estimación de riesgos para la EEQ, tenga un enfoque cualitativo tanto para la probabilidad como para el impacto, debido a que es la primera iniciativa que se ejecuta en cuanto a gestión de riesgos de seguridad de la información, por tanto no hay referencias a otros procesos ni datos históricos que provean guías para la definición de las escalas de probabilidad e impacto.

4.3.2.2.3.2 Resultado obtenido

Resultados de determinar la metodología de estimación del riesgo					
Metodología de estimación del riesgo					
Enfoque	Cualitativo				
Justificación	Es la primera iniciativa que se ejecuta en cuanto a gestión de riesgos de seguridad de la información, por tanto no hay referencias a otros procesos ni datos históricos que provean guías para la definición de las escalas de probabilidad e impacto				
Escala de probabilidad	Alta		Media		Baja
Escala de impacto	Alta		Media		Baja
Estimación del riesgo en base a	Matriz de valor esperado				
			Probabilidad		
			Alta	**Media**	**Baja**
	Impacto	**Alto**	Alto	Alto	Medio
		Medio	Alto	Medio	Bajo
		Bajo	Medio	Bajo	Bajo
Observaciones	Para llegar a a definir la metodología de estimación del riesgo fue necesario reforzar el conocimiento del equipo de análisis en el contexto de riesgos en base al marco conceptual del modelo de gestión de riesgos de seguridad de la información.				
Fecha	16-jul-12				
Realizado por	El equipo de análisis				

Resultado 4.3-7 Determinar la metodología de estimación del riesgo

Fuente: Los autores

4.3.2.2.3.3 Observaciones

Se ha visto necesario que el equipo de análisis requería tener conocimiento en manejo de riesgos, de acuerdo a definir la metodología de estimación de riesgos que más le convenga a la EEQ. Por lo que fue necesario reforzar el conocimiento del equipo de análisis, aún más allá de lo ofrecido por la guía de implementación.

4.3.2.2.3.4 Recomendaciones

Dado que el contexto de los riesgos de seguridad de la información, es por naturaleza complejo, es necesario considerar el tener acceso a consultores expertos que apoyen en la clarificación de los criterios a tomar en cuenta en la definición de una metodología de estimación del riesgo.

4.3.2.2.4 Actividad 7: Definir el criterio básico de evaluación de riesgo

4.3.2.2.4.1 Detalle de ejecución

El equipo de análisis convocó a los participantes a un taller de acuerdo a definir el criterio básico de evaluación de riesgo, en esta reunión se cumplimentó una plantilla predefinida con criterios correspondientes a las mejores prácticas, como el valor estratégico de los procesos del negocio, requerimientos legales y contractuales, expectativas y percepción de los interesados; se validó la aplicabilidad de estos criterios respecto al plan estratégico. Se utilizó la escala de impacto cualitativa, acorde a la metodología de estimación de riesgo. Adicionalmente se analizó cuales de estas áreas aplicaban la EEQ, se procedió a llenar los criterios.

Se realizó un taller posterior con la alta directiva, de acuerdo a afinar los criterios definidos por los participantes de los talleres. En este taller se realizó una inducción respecto al marco conceptual de riesgos de seguridad de la información.

4.3.2.2.4.2 Resultado obtenido

Resultados de definición de criterio básico de evaluación de riesgo			
Criterio	**Bajo**	**Medio**	**Alto**
Valor estratégico de los procesos del negocio	Procesos de apoyo.	Procesos de gestión de estratégica corporativa.	Procesos de gestión de la energía desde la oferta y la demanda. Procesos de gestión de servicios al cliente.
Requerimientos legales y contractuales	Reglamento de Tarifas. Reglamento Ambiental para Actividades Eléctricas. Reglamento para la Administración del Fondo de Electrificación Rural-Urbano Marginal, FERUM. Ordenanzas Municipales. Regulaciones del CONELEC.	Código Orgánico de Planificación y Finanzas Públicas. Código Orgánico de Organización Territorial, Autonomía y Descentralización. Código del Trabajo.Ley Orgánica de Empresas Públicas. Ley Orgánica del Servicio Público. Ley Orgánica de Defensa del Consumidor. Ley Orgánica de Transparencia y Acceso a la Información Pública. Ley de Gestión Ambiental. Ley para la constitución de gravámenes y Derechos tendientes a Obras de Electrificación. Ley Orgánica del Sistema Nacional de Contratación Pública.	Constitución. Plan Nacional para el Buen Vivir. Agenda Estratégica y Modelo de Gestión del Sector Eléctrico. Ley de Empresas Públicas.
Expectativas y percepción de los interesados (consumidores, comunidad, colaboradores, proveedores).	Adecuado ambiente laboral. Compromiso social. Ley de Contratación Pública. Calidad de servicio comercial.	Uso responsable de la Electricidad y respeto al ambiente. Eficiencia y diversificación energética. Control de pérdidas. Eficiencia en la gestión financiera. Generación de electricidad. Cobertura de demanda de la electricidad. Alumbrado público. Calidad de suministro de energía y mejoramiento de la Infraestructura eléctrica.	Mejoramiento de los sistemas transaccionales de gestión y estratégicos. Transparencia y rendición de cuentas. Mejoramiento de procesos.
Observaciones			
Fecha	23-jul-12		
Realizado por	Equipo de análisis		

Resultado 4.3-8 Definición de criterio básico de evaluación de riesgo

Fuente: Los autores

4.3.2.2.4.3 Observaciones

No se encontró criterios de evaluación de riesgos, adicionales a los criterios recomendados por las mejores prácticas.

4.3.2.2.4.4 Recomendaciones

Es recomendable utilizar plantillas predefinidas con los criterios correspondientes a las mejores prácticas. Adicionalmente, es importante validar los criterios predefinidos de acuerdo al plan estratégico.

4.3.2.2.5 Actividad 8: Definir el criterio básico de impacto

4.3.2.2.5.1 Detalle de ejecución

El equipo de análisis convocó a los participantes a un taller de acuerdo a definir el criterio básico de impacto, en esta reunión se cumplimentó una plantilla predefinida con criterios correspondientes a las mejores prácticas como confianza del cliente, financiera, productividad, seguridad y salud, multas y penalidades legales; se validó la aplicabilidad de estos criterios respecto al plan estratégico. Se utilizó la escala de impacto cualitativa, acorde a la metodología de estimación de riesgo. Adicionalmente se analizó cuales de estas áreas aplicaban la EEQ, se procedió a llenar los criterios y priorizarlos.

Se realizó un taller posterior con la alta directiva, de acuerdo a afinar los criterios y la priorización realizada por los participantes de los talleres. En este taller se realizó una inducción respecto al marco conceptual de riesgos de seguridad de la información.

4.3.2.2.5.2 Resultado obtenido

Resultado de definición de criterio básico de impacto			
Imagen y confianza del cliente			
Área de Impacto	**Baja**	**Media**	**Alta**
Imagen	La imagen se ve mínimamente afectada, o un pequeño esfuerzo o gasto es requerido para su recuperación.	La imagen se ve afectada y muchos esfuerzos y gastos son requeridos para su recuperación.	La imagen se ve irrevocablemente destruida o afectada.
Satisfacción del cliente	ISCAL mayor o igual al 70%.	ISCAL mayor o igual al 50% y menor o igual al 70%.	ISCAL menor al 50%.
Financiero			
Área de Impacto	**Baja**	**Media**	**Alta**
Costos de Operación	Aumento de hasta 5% en costos de operaciones anualmente.	Aumento de 5% al 5.81% en costos de operaciones anualmente.	Aumento mayor al 5.81% en costos de operaciones anualmente.
Pérdidas de Ingresos	La recaudación podría disminuir hasta en 5x1000 mensualmente.	La recaudación podría disminuir hasta en 10x1000 mensualmente.	la recaudación podría disminuir mas del 10x1000 mensualmente.
Productividad			
Área de Impacto	**Baja**	**Media**	**Alta**
Sobretiempos	El incremento en sobretiempos del 5% mendualmente	Aumento de sobretiempos desde el 5% hasta 20% mensualmente	Aumento de sobretiempos mayor al 20% mensualmente.
Contrataciones Complementarias de servicios (ampliaciones de contratos)	Mas del 10% de ampliaciones de contratos anualmente	Del 10% al 20% de ampliaciones de contrato anualmente	Mas del 20% de ampliaciones de contrato anualmente
Seguridad y Salud			
Área de Impacto	**Baja**	**Media**	**Alta**
Vida	Sin pérdidas o amenazas no significativas para la vida de los clientes o miembros del personal.	La vida de los clientes o miembros del personal están amenazada pero se recuperarán después de recibir tratamiento médico	Pérdida de vidas de los clientes o miembros del personal.
Salud	Mínima, degradación tratable inmediatamente en la salud de los clientes o miembros del personal con recuperación dentro de cuatro días.	Incapacidad temporal o recuperable de la salud de los clientes o miembros del personal.	Discapacidad permanente de aspectos significativos de la salud de los clientes o miembros del personal.
Seguridad	Seguridad cuestionada	Seguridad afectada	Seguridad Violada
Multas y penalidades legales			
Área de Impacto	**Baja**	**Media**	**Alta**
Multas y sanciones	No existen sanciones superiores a 5% de la facturación mensual promedio del último año fiscal	Existen sanciones económicas superiores al 5% pero inferiores al 20% de la facturación mensual promedio del último año fiscal	Existen sanciones económicas superiores al 20% de la facturación mensual promedio del último año fiscal
Demandas	No hay demandas	Existen menos de 5 demandas planteadas sobre el tema	Hay más de 5 demandas planteadas sobre el tema
Observaciones de entidades de control y autoridades competentes	No existen consultas desde el gobierno u otras organizaciones investigativas.	El gobierno u otras organizaciones investigativas solicitan información o registros (no amplias).	El gobierno u otras organizaciones investigativas inician investigaciones amplias y profundas dentro de las prácticas organizacionales.
Observaciones			
Fecha	30-jul-12		
Realizado por	Equipo de análisis		

Resultado 4.3-9 Definición de criterio básico de impacto

Fuente: Los autores

4.3.2.2.5.3 Observaciones

No se encontró criterios de impacto nuevos adicionales a los criterios recomendados por las mejores prácticas.

4.3.2.2.5.4 Recomendaciones

Es recomendable utilizar plantillas predefinidas con los criterios correspondientes a las mejores prácticas. Adicionalmente, es importante validar los criterios predefinidos de acuerdo al plan estratégico y sus indicadores.

4.3.2.2.6 Actividad 9: Definir el criterio básico de aceptación de riesgo

4.3.2.2.6.1 Detalle de ejecución

El equipo de análisis convocó a los participantes a un taller de acuerdo a definir el criterio de aceptación del riesgo, en esta reunión se realizó un análisis utilizando la escala de nivel de riesgo cualitativa, acorde a la metodología de estimación de riesgo. Posteriormente se analizó cuales de estos niveles y bajo qué condiciones pueden ser aceptados.

Se realizó un taller posterior con la alta directiva, de acuerdo a afinar los criterios.

4.3.2.2.6.2 Resultado obtenido

Resultados de definición del criterio básico de aceptación del riesgo		
Nivel de riesgo estimado	**Criterio de aceptación**	**Descripción**
Alto	No se acepta	Al no ser aceptado, se debe optar por una opción de tratamiento para la mitigación. Se definirán los planes y acciones correspondientes.
Medio	No se acepta, requiere un análisis más profundo de la naturaleza de este riesgo en base a su probabilidad e impacto.	Al no ser aceptado, se debe optar por una opción de tratamiento para la mitigación. Se definirán los planes y acciones correspondientes.
Bajo	Se acepta	Riesgo retenido, sin más acciones al respecto.
Observaciones		
Fecha	06-ago-12	
Realizado por	Equipo de análisis	

Resultado 4.3-10 Criterio básico de aceptación del riesgo

Fuente: Los autores

4.3.2.2.6.3 Observaciones

El criterio de aceptación de riesgo será una referencia inicial respecto de la aceptación o mitigación del riesgo en base al riesgo estimado, sin embargo será necesario realizar análisis más profundos en los casos de riesgos estimados medios, debido a que pueden provenir de varios contextos.

4.3.2.2.6.4 Recomendaciones

Es recomendable utilizar plantillas predefinidas con los criterios de aceptación de riesgo en base a las escalas propuestas en la metodología de estimación de riesgo.

4.3.2.2.7 Actividad 10: Definir la organización para la gestión de riesgos de seguridad de la información

4.3.2.2.7.1 Detalle de ejecución

Dos de los integrantes del equipo de análisis pertenecen a la organización para la gestión de riesgos de seguridad de la información, que actualmente existe en la EEQ. De acuerdo a esto, no fue necesario crear esta organización. Sin embargo, se realizó una revisión y ajuste de los roles, responsabilidades, establecimiento de las relaciones entre la organización y interesados, interfaces hacia los más altos niveles de funciones de gestión de riesgos, definición de caminos de escalamiento de decisión.

4.3.2.2.7.2 Resultado obtenido

Resultados de definición de la organización para la gestión de riesgos de seguridad de la información		
Organización de seguridad de la información		
Nombre	Sección de seguridad de la información	
Integrantes		
Apellidos	**Nombres**	**Cargo**
Carrera	Walter	Jefe de sección de Seguridad de la información
García	Santiago	Ingeniero en sistemas
Rol	Gestionar los riesgos de seguridad de la información de la Empresa Eléctrica Quito.	
Responsabilidades	Identificará los riesgos de seguridad de la información.	
Relaciones con la organización e interesados	La organización de riesgos de seguridad de la información, actualmente está conformada, sin embargo está bajo la Dirección de TIC, de acuerdo a esto, se solicitará a la alta directiva que esta organización sea un ente independiente de TI.	
Interfaces hacia los altos niveles	Actualmente la organización de gestión de seguridad de la información, de acuerdo a comunicarse a los más altos nieles debe hacerlo a través de la Dirección de Tecnología de información y comunicaciones hasta la Gerencia de Planificación.	
Caminos de escalamiento de decisión	Actualmente la organización de gestión de seguridad de la información, de acuerdo a escalar las decisiones pasa por hasta 3 niveles de escalamiento.	
Observaciones		
Fecha	16-ago-12	
Realizado por	Equipo de análisis	

Resultado 4.3-11 Definición de la organización de gestión de riesgos de seguridad de la información

Fuente: Los autores

4.3.2.2.7.3 Observaciones

Se encontró que la organización para la gestión de riesgos de seguridad de la información forma parte de la Dirección de tecnología de la información y comunicaciones. Esto no es lo recomendable, pues esta organización pierde independencia en su gestión, en relación al área de TI.

4.3.2.2.7.4 Recomendaciones

Sugerir a la alta directiva un proceso de separación de la organización para la gestión de riesgos de seguridad de la información de la Dirección de tecnología de la información y comunicaciones.

4.3.2.3 Proceso de identificación de riesgos

4.3.2.3.1 Actividad 11: Identificar activos

4.3.2.3.1.1 Detalle de ejecución

El equipo de análisis organizó un taller con los participantes, donde se identificó aquellos activos que utilizan para ayudar a la organización en el cumplimiento de su misión y objetivos. Se tasó los activos de acuerdo a su importancia acorde a la

consecuencia relacionada a la revelación, modificación, pérdida o interrupción de información.

Se utilizó una escala de valoración cuantitativa con el propósito de ordenar de mayor a menor la importancia, y de acuerdo a esto establecer la prioridad. Se eligió los 5 activos (críticos) con tasaciones más altas.

4.3.2.3.1.2 Resultado obtenido

Resultados de identificación de activos					
Activo	**Razón de selección**	**Descripción acordada**	**Propietario**	**Categoría**	**Prioridad (tasación)**
Sistema de facturación	Este sistema permite aplicar los pliegos tarifarios, procesar crítica de lecturas, calcular los conceptos a facturar, determinar montos elevados, generar movimientos contables, generar las facturas, realizar refacturaciones.	Sieeq Comercial	Sección de desarrollo de sistemas administrativos	Sistema	12
Datamart Facturación	Este sistema de apoyo a la toma de decisiones a cerca del proceso de facturación.	Datamart	Sección de desarrollo de sistemas administrativos	Sistema	10
Sidebench	Este sistema muestra indicadores de desempeño a cerca de las lecturas, reparto de facturas, refacturaciones, etc.	Sidebench	Sección de desarrollo de sistemas administrativos	Sistema	8
Sistema de toma de lecturas	Este sistema permite a los lectores reportar las lecturas obtenidas en trabajo en el campo.	Sistema móvil de lecturas	Sección de desarrollo de sistemas administrativos	Sistema	9

Resultado 4.3-12 Identificación de activos

Fuente: Los autores

La identificación de activos completa, puede encontrarse en el Anexo 7.

Activos críticos
Sieeq Comercial
Personal de tratamiento de facturación
Datamart
Sistema móvil de lecturas
Sidebench

Resultado 4.3-13 Activos críticos

Fuente: Los autores

4.3.2.3.1.3 Observaciones

Se considera que la categoría de sistema, se constituye de activos de información, software y hardware.

4.3.2.3.1.4 Recomendaciones

Con el propósito de tasar los activos es recomendable direccionar a los participantes en pensar en cómo se vería afectadas sus actividades al sufrir una revelación, modificación, pérdida o interrupción de información. El siguiente paso en este contexto y de acuerdo a priorizar los activos, es necesario que los participantes estimen que activo es más importante que otro, o con cuál de estos de algún modo se puede prescindir.

4.3.2.3.2 Actividad 12: Identificar las áreas de interés

4.3.2.3.2.1 Detalle de ejecución

El equipo de análisis organizó dos talleres con los participantes, donde se identificó para cada uno de los cinco activos críticos, los escenarios que los ponen en peligro. Se utilizó las fuentes típicas de amenaza accidentales o deliberadas (actores humanos con acceso a red, actores humanos con acceso físico, problemas del sistema y otros problemas) y sus resultados (revelación, modificación, pérdida o interrupción de la información). Adicionalmente se determinó por cada escenario, el impacto (lo que pasaría si efectivamente este ocurre).

4.3.2.3.2.2 Resultado obtenido

Resultados de identificar las áreas de interés				
Sieeq Comercial				
Fuente de amenaza	**Nro.**	**Área de interés**	**Resultado**	**Impacto**
Acciones deliberadas o accidentales por personas	1	Personal alterando facturas, pliegos tarifarios de forma no autorizada.	Modificación	Multas por parte de los entes reguladores. Reclamos de los clientes a cerca de sus facturas. Pérdidas económicas para la EEQ. Pérdida de productividad.
	2	Personal ingresando erróneamente parámetros para la facturación.	Modificación	Reclamos de los clientes a cerca de sus facturas.
	3	Personal accediendo a información a la que no debería tener acceso.	Revelación	Multas por parte de los entes reguladores. Reclamos de los clientes a cerca de sus facturas. Daño a la imagen de la EEQ. Pérdidas económicas para la EEQ. Pérdida de productividad.
	4	Las personas no bloquean sus pantallas con contraseña	Revelación	Reclamos de los clientes. Daño a la imagen de la EEQ. Pérdida de productividad.
	5	Las personas comparten sus contraseñas.	Revelación	Reclamos de los clientes. Daño a la imagen de la EEQ.
	6	Vulnerabilidades tecnológicas en el sistema podrían ser explotadas	Modificación Destrucción	Daño a la imagen de la EEQ.
	7	Los desarrolladores conocen la contraseña del esquema de base de datos de producción	Modificación	Alteración de la integridad de la información.

Resultado 4.3-14 Identificar áreas de interés

Fuente: Los autores

La identificación de áreas de interés completa, puede encontrarse el Anexo 7.

4.3.2.3.2.3 Observaciones

Se encontró más de un impacto (lo que pasaría si efectivamente este ocurre) para cada área de interés.

4.3.2.3.2.4 Recomendaciones

Es recomendable analizar en orden las fuentes típicas de amenaza por cada activo, de este modo se lleva control de las que se ha completado exitosamente.

4.3.2.3.3 Actividad 13: Identificar los requisitos de seguridad

4.3.2.3.3.1 Detalle de ejecución

El equipo de análisis organizó talleres con los participantes, donde se identificó para cada uno de los cinco activos críticos, las descripciones narrativas acerca de los requisitos de seguridad, asociados a la confidencialidad, integridad y disponibilidad. Posteriormente se eligió el requisito más importante por activo.

4.3.2.3.3.2 Resultado obtenido

Resultados de requisitos de seguridad			
Requisitos de seguridad			
Activo	**Confidencialidad**	**Integridad**	**Disponibilidad**
Sieeq Comercial	La información a cerca de datos de los abonados, facturas deben mantenerse confidenciales, restringida a lo que cada perfil requiere acceder	Los registros deben mantenerse exactos y completos. Únicamente los usuarios autorizados pueden alterar la información, de acuerdo a su perfil.	*La información se requiere en un esquema 24x7, pues los procesos de facturación así lo requieren.
Personal de tratamiento de facturación	No aplica	No aplica	* El personal de tratamiento de facturación debe estar disponible para ejecutar sus procesos diarios dentro de cada ciclo de facturación.
Datamart	La información de toma de decisiones del Datamart es estrictamente confidencial, restringida a los perfiles que tengan concedido el acceso.	*La información de toma de decisiones del Datamart debe mantenerse exacta y completa, nadie puede alterar esta información.	* El Datamart debe estar disponible en un esquema 24x7.
Sistema móvil de lecturas	La información generada a través del sistema móvil de lecturas debe mantenerse confidencial, restringida a los perfiles que tengan concedido el acceso.	*La información generada a través del sistema móvil de lecturas debe mantenerse exacta y completa, nadie debe alterar esta información.	El sistema de lecturas debe estar disponible en cada PocketPC en un esquema 24x7.
Sidebench	La información de los índices de gestión es estrictamente confidencial, restringida a los perfiles que tengan concedido el acceso.	*La información de los índices de gestión debe mantenerse exacta y completa, nadie puede alterar esta información.	Sidebench debe estar disponible en un esquema 24x7.
Observaciones	Por cada activo, el requisito de seguridad marcado con * es el más importante.		
Fecha	03-sep-12		
Realizado por	El equipo de análisis		

Resultado 4.3-15 Requisitos de seguridad

Fuente: Los autores

4.3.2.3.3.3 Observaciones

Se determinó una sola narración descriptiva por cada requisito de seguridad.

4.3.2.3.3.4 Recomendaciones

Considerar que generalmente los requisitos de confidencialidad no aplican para activos de HW y SW. Y para los activos de tipo persona únicamente aplica la disponibilidad.

4.3.2.3.4 Actividad 14: Identificar controles existentes.

4.3.2.3.4.1 Detalle de ejecución

Se organizó un taller para los participantes del proceso de facturación y área legal de la organización para determinar el cumplimiento de los controles propuestos por la norma ISO/IEC 27002:2005. Los dominios tratados en este taller no eran de índole tecnológica. Sin embargo, estos dominios se trataron en otro taller únicamente para miembros de la Dirección de tecnología de información y comunicaciones.

4.3.2.3.4.2 Resultado obtenido

Resumen de controles existentes	
Controles por dominio	
No se cumple con los controles asociados a los dominios de política de seguridad, gestión de activos, adquisición desarrollo y mantenimiento de los sistemas de información, gestión de índices de seguridad, gestión de continuidad de negocio.	
Se cumple parcialmente los controles asociados a aspectos organizativos de la seguridad de la información, los dominios de seguridad ligada a recursos humanos, seguridad física y ambiental, gestión de comunicaciones y operaciones, control de accesos, y cumplimiento.	
Hallazgos principales	
No se pudo evidenciar la existencia de una política de seguridad de información que se encuentre aprobada y difundida	
No se pudo evidenciar la existencia de un inventario de activos de información, procedimiento de clasificación y asignación de dueños de datos, tampoco se cuenta con una metodología para realizar un análisis de riesgos y poder realizar un tratamiento de los riesgos.	
Existe poca documentación de Normas, Estándares, Instructivos de Seguridad, Procedimientos Operativos Diarios, que han sido desarrollados, aprobados y difundidos al interior de la EEQ.	
No se cuenta con un Plan de Continuidad de Negocios.	
Observaciones	
Fecha	12-sep-12
Realizado por	El equipo de análisis

Resultado 4.3-16 Resumen de controles existentes

Fuente: Los autores

El detalle de cada uno de los controles se puede observar en el Anexo 7.

4.3.2.3.4.3 Observaciones

Se encontró muchos aspectos por mejorar en todos los dominios, esto indica que hay muy pocos controles aplicados de forma efectiva de acuerdo a la norma.

4.3.2.3.4.4 Recomendaciones

Generar un resumen de la encuesta por dominios para clarificar los resultados.

Previo al taller, es recomendable realizar una inducción respecto a los dominios y controles de la norma.

4.3.2.3.5 Actividad 15: Identificar amenazas

4.3.2.3.5.1 Detalle de ejecución

El equipo de análisis mapeó las áreas de interés hacia los componentes de las propiedades de amenaza que son activo, acceso, actor, motivo y resultado. Esta tarea la realizó por activo. Al realizar esta tarea se reconoció que en las categorías de amenaza asociadas a problemas de sistema y otros problemas, se generaron nuevos actores que no estaban contemplados en el perfil genérico de riesgo (ver Anexo 4). De acuerdo a esto, se procedió a incorporar estos actores en el perfil genérico de riesgo, generando así el Perfil genérico de riesgo para EEQ que se encuentra en el Anexo 5.

Posteriormente, el equipo de análisis trasladó los componentes de amenaza a los árboles del perfil genérico de amenaza para la EEQ, para las categorías de amenaza que aplican para cada caso. Se revisó también el catálogo de amenazas y vulnerabilidades proporcionado por la norma ISO/IEC 27005:2008 en su Anexo C y D respectivamente, con el propósito de encontrar nuevas amenazas no detectadas al momento.

A continuación, se realizó un análisis de brechas de los perfiles de amenaza generados, revisando la consistencia, es decir, se realizó una verificación de asociación entre los requisitos de seguridad y las categorías de resultados esperados, por ejemplo de forma general un área de interés asociada a un comprometimiento de la confidencialidad, debería asociarse a un resultado de revelación (ver tabla 3-13). Adicionalmente se verificó los tipos de amenazas aplicables por cada tipo de activo, por ejemplo para los tipos de activo asociados a personas aplica únicamente la categoría de amenaza de otro problemas (ver tabla 3-14).

Finalmente, se revisó todos los árboles de amenaza generados, buscando casos en los que un resultado implique a otro, por ejemplo se encontró que por una pérdida de energía se puede interrumpir el servicio brindado por un componente, pero adicionalmente, este componente podría ser irrecuperable, es decir aplicaría también un resultado de pérdida o destrucción.

4.3.2.3.5.2 Resultado obtenido

Activo: Sieeq Comercial **Mapeo de áreas de interés a propiedades de amenaza**		
Área de Interés	**Activo**	Sieeq Comercial
1. Personal alterando pliegos tarifarios de forma no autorizada.	**Acceso**	Red
	Actor	Interno
	Motivo	Deliberado
	Resultado	Modificación
Área de Interés	**Activo**	Sieeq Comercial
2. Personal ingresando erróneamente parámetros para la facturación.	**Acceso**	Red
	Actor	Interno
	Motivo	Accidental
	Resultado	Modificación
Área de Interés	**Activo**	Sieeq Comercial
3. Personal accediendo a información a la que no debería tener acceso.	**Acceso**	Red
	Actor	Interno
	Motivo	Deliberado
	Resultado	Revelación

Resultado 4.3-17 Identificar Amenazas

Fuente: Los autores

El mapeo de áreas de interés completo, se puede observar en el Anexo 7.

Árbol de amenaza basado en activo para Actores humanos utilizando la red

Activo	Acceso	Actor	Motivo	Resultado	Área de Interés
Sieeq Comercial	Red	Interno	Accidental	Revelación	
				Modificación	2, 7
				Pérdida	
				Interrupción	
			Deliberado	Revelación	3, 5
				Modificación	1, 6
				Pérdida	6
				Interrupción	
		Externo	Accidental	Revelación	
				Modificación	
				Pérdida	
				Interrupción	
			Deliberado	Revelación	
				Modificación	6
				Pérdida	6
				Interrupción	

Observaciones	
Fecha	17-sep-12
Realizado por	El equipo de análisis

Resultado 4.3-18 Árbol de amenaza Sieeq Comercial (acceso Red)

Fuente: Los autores

El resto de árboles de amenaza se puede observar en el Anexo 7.

4.3.2.3.5.3 Observaciones

En los árboles de amenaza:

- Las ramas de línea continua con área de interés: amenazas potenciales mapeadas de las áreas de interés.
- Las ramas de línea continua sin áreas de interés: inicialmente no eran riesgo, sin embargo, luego del análisis de brechas, se determinó que si existía una posibilidad de amenaza al activo.
- Las ramas de línea punteada, no representan riesgo.

4.3.2.3.5.4 Recomendaciones

Es recomendable, preparar una ayuda con el objetivo de que se pueda comprender los árboles de amenaza, indicando el significado de las líneas continuas sin área de interés, con áreas de interés y las líneas entre cortadas.

4.3.2.3.6 Actividades 16 y 17: Seleccionar los componentes de la infraestructura a evaluar e Identificar vulnerabilidades tecnológicas

4.3.2.3.6.1 Detalle de ejecución

El equipo de análisis en acuerdo con el comité de seguridad de la información ha acordado manejar la selección y evaluación de vulnerabilidades tecnológicas como un proyecto independiente que se ejecute con el apoyo de expertos externos especialistas en test de intrusión. Este proyecto se realiza como apoyo al modelo de gestión de riesgos de seguridad de la información. Para lograr este objetivo se ha incluido dentro del alcance del proyecto a los componentes tecnológicos asociados a los activos críticos detectados en actividades anteriores.

4.3.2.3.6.2 Resultado obtenido

No aplica.

4.3.2.3.6.3 Observaciones

Se ha opado por contratar expertos externos en test de intrusión debido a la falta de experiencia y conocimiento del personal de tecnología de la información en este tipo de actividades.

4.3.2.3.6.4 Recomendaciones

Se recomienda incluir como objetivo del proyecto de test de intrusión la incorporación de las recomendaciones generadas por este proyecto en los planes de tratamiento al riesgo de la EEQ.

4.3.2.4 Proceso de evaluación de riesgos

4.3.2.4.1 Actividad 18: Identificar impacto

4.3.2.4.1.1 Detalle de ejecución

El equipo de análisis, a través de talleres con los participantes, identificó narraciones descriptivas asociadas a las áreas del criterio básico de impacto. Esta actividad se realizó por cada uno de los activos críticos en relación a los resultados de revelación, modificación pérdida e interrupción. Se revisó todos los perfiles de amenaza identificando aquellos resultados que apliquen para la categoría de activo.

4.3.2.4.1.2 Resultado obtenido

Resultado de identificar impacto	
Sieeq Comercial	
Resultado	**Descripción de Impacto**
Revelación	Imagen: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en una grave afectación de la imagen de la EEQ.
	Satisfacción del cliente: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en reclamos de los clientes, provocando una reducción de su satisfacción.
	Costos de Operación: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, no podría resultar en un aumento de los costos de operación.
	Pérdida de Ingresos: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, no podría resultar en una pérdida de ingresos.
	Sobretiempos: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, no podría resultar en un incremento de los sobretiempos del personal.
	Contrataciones complementarias de servicios: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, no podría resultar en realizar contrataciones complementarias.
	Vida: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría afectar la vida de los clientes en caso de que la información llegue a manos de delincuentes.
	Salud: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría afectar significativamente la salud de los clientes en caso de que la información llegue a manos de delincuentes.
	Seguridad: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría afectar la seguridad de los clientes en caso de que la información llegue a manos de delincuentes.
	Multas y Sanciones: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en un multas por parte de los entes reguladores.
	Demandas: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en demandas por parte de los clientes a causa de divulgar información personal.
	Observaciones de entidades de control y autoridades competentes: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en investigaciones a la EEQ por parte de los entes reguladores.

Resultado 4.3-19 Identificar Impacto Sieeq Comercial

Fuente: Los autores

La identificación de impactos completa puede encontrarse en el Anexo 7.

4.3.2.4.1.3 Observaciones

Se encontró criterios de impacto que no tenían ninguna relación con los resultados para un determinado activo crítico, a estos casos se les calificará posteriormente como bajo impacto.

4.3.2.4.1.4 Recomendaciones

Considerar que no todos los resultados aplican a todo tipo de activo, por ejemplo para activo de tipo persona generalmente aplica la interrupción, en relación a la disponibilidad de la persona. Sin embargo se debe realizar el análisis de la aplicabilidad de los otros resultados.

4.3.2.4.2 Actividad 19: Valorar el impacto de las amenazas

4.3.2.4.2.1 Detalle de ejecución

El equipo de análisis, a través de talleres con los participantes, valoró el impacto a las amenazas a través de la comparación de las descripciones narrativas de impacto

descritas en la sección anterior con el criterio de básico de impacto. Es decir, a cada una de las narraciones descriptivas, por activo y por resultado, se les asignó un valor de acuerdo a la escala propuesta en el criterio básico de impacto. De acuerdo a esto, cada resultado por cada área de impacto contó con una valoración, para el caso Alta, Media o Baja.

4.3.2.4.2.2 Resultado obtenido

Resultado de valorar impacto		
Sieeq Comercial		
Resultado	**Descripción de Impacto**	**Valor de Impacto**
Revelación	Imagen: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en una grave afectación de la imagen de la EEQ.	A
	Satisfacción del cliente: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en reclamos de los clientes, provocando una reducción de su satisfacción.	M
	Costos de Operación: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, no podría resultar en un aumento de los costos de operación.	B
	Pérdida de Ingresos: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, no podría resultar en una pérdida de ingresos.	B
	Sobretiempos: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, no podría resultar en un incremento de los sobretiempos del personal.	B
	Contrataciones complementarias de servicios: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, no podría resultar en realizar contrataciones complementarias.	B
	Vida: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría afectar la vida de los clientes en caso de que la información llegue a manos de delincuentes.	A
	Salud: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría afectar significativamente la salud de los clientes en caso de que la información llegue a manos de delincuentes.	A
	Seguridad: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría afectar la seguridad de los clientes en caso de que la información llegue a manos de delincuentes.	A
	Multas y Sanciones: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en un multas por parte de los entes reguladores.	M
	Demandas: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en demandas por parte de los clientes a causa de divulgar información personal.	M
	Observaciones de entidades de control y autoridades competentes: Una falla en salvaguardar la privacidad de la información del cliente como sus datos personales o de facturas, podría resultar en investigaciones a la EEQ por parte de los entes reguladores.	A

Resultado 4.3-20 Impacto valorado Sieeq Comercial

Fuente: Los autores

La valoración de impacto completa, puede encontrarse en el Anexo 7.

Árbol de amenaza basado en activo para Actores humanos utilizando la red

Activo	Acceso	Actor	Motivo	Resultado	Área de Interés	Impacto
Sieeq Comercial	Red	Interno	Accidental	Revelación		
				Modificación	2, 7	A-M-B
				Pérdida		A-M-B
				Interrupción		M-B
			Deliberado	Revelación	3, 5	A-M-B
				Modificación	1, 6	A-M-B
				Pérdida	6	A-M-B
				Interrupción		M-B
		Externo	Accidental	Revelación		
				Modificación		
				Pérdida		
				Interrupción		
			Deliberado	Revelación		A-M-B
				Modificación	6	A-M-B
				Pérdida	6	A-M-B
				Interrupción		M-B

Observaciones	
Fecha	01-oct-12
Realizado por	El equipo de análisis

Resultado 4.3-21 Perfil de riesgo Sieeq Comercial (acceso red)

Fuente: Los autores

Los perfiles de riesgo con impacto valorado, completos pueden encontrarse en el Anexo 7.

*4.3.2.4.2.3*Observaciones

Debido a que hay varias áreas de impacto en el criterio básico de impacto, se obtuvo varias valoraciones por cada tipo de resultado y para cada activo, de acuerdo a esto, fue necesario establecer rangos de valoración, por ejemplo al tener varias valoraciones de altos, medios y bajos, la valoración global sería un rango de alto a medio a bajo. Para facilidad de manejo de la valoración, los rangos se expresan con los acrónimos A, M, y B separados por un guión "-". Por ejemplo; A-M-B.

4.3.2.4.2.4 Recomendaciones

Para los casos de criterios de impacto que no tenían ninguna relación con los resultados para un determinado activo crítico, se les valoró como Bajo.

4.3.2.4.3 Actividad 20: Describir la probabilidad de amenazas

4.3.2.4.3.1 Detalle de ejecución

El equipo de análisis, a través de talleres con los participantes, revisó todos los perfiles de riesgo, definiendo para cada uno de ellos los motivos, medios, oportunidad, circunstancias inusuales y datos históricos que le permitan recabar datos subjetivos y objetivos con el propósito de establecer la caracterización de la probabilidad (frecuencia de ocurrencia) de los riesgos analizados. Este análisis se realizó por cada rama con riesgo de todos los perfiles de riesgo.

Para cada una de los componentes de descripción de probabilidad, se utilizó narraciones descriptivas.

4.3.2.4.3.2 Resultado obtenido

Resultado de describir probabilidad de amenaza					
Sieeq Comercial					
Acceso	**Actor**	**Motivo**	**Resultado**	**Descripción de probabilidad**	
Red	Interno	Accidental	Modificación Pérdida Interrupción	**Motivos**	Accidental.
				Recursos	Redes Wifi, equipos de usuarios.
				Oportunidad	Contraseñas débiles en el sistema.
				Circunstancias inusuales de afectación	Asignación errada de perfiles a usuarios.
				Referencias a datos históricos	Ninguna.
Red	Interno	Deliberado	Revelación Modificación Pérdida Interrupción	**Motivos**	Empleados que quieren causar daño por resentimiento
				Recursos	Redes Wifi, equipos de usuarios.
				Oportunidad	Contraseñas débiles en el sistema.
				Circunstancias inusuales de afectación	Publicación de clientes de bases de datos en los equipos de usuarios.
				Referencias a datos históricos	Ninguna.

Resultado 4.3-22 Describir probabilidad de amenaza Sieeq Comercial

Fuente: Los autores

La descripción de probabilidad para las amenazas, completas, puede encontrarse en el Anexo 7.

4.3.2.4.3.3 Observaciones

Únicamente se encontró datos objetivos que hacen referencia los perfiles de riesgo de problemas de sistema y otros sistemas, pues en la EEQ, mucha de esta referencia se pudo ubicar en el sistema de mesa de ayuda. Sin embargo, para los casos de accesos humanos vía red o físico no se encontró ninguna información.

4.3.2.4.3.4 Recomendaciones

Utilizar los sistemas informáticos de gestión de incidentes y problemas, en busca de información histórica de eventos.

4.3.2.4.4 Actividad 21: Definir el criterio de probabilidad

4.3.2.4.4.1 Detalle de ejecución

El equipo de análisis, a través de talleres con los participantes, determinó las escalas de valoración de probabilidad, como alta, media y baja. Esta elección se realizó en concordancia con los lineamientos dispuestos en la metodología de estimación de riesgos.

Adicionalmente, definió el criterio de probabilidad en base a las descripciones de probabilidad establecidas en la actividad anterior, la complejidad de esta tarea y la falta de datos históricos hizo necesario un análisis a detalle de cada uno de los perfiles riesgo, es decir, se generó un criterio de probabilidad individual para cada riesgo, para posteriormente generar un criterio de probabilidad único que sea congruente con todos ellos.

4.3.2.4.4.2 Resultado obtenido

Resultado de definir criterio de probabilidad	
	Criterio de probabilidad
Alto	Más de 2 veces al año.
Medio	De 1 a 2 veces al año.
Bajo	Menos de 1 vez al año.
Observaciones	
Fecha	12-oct-12
Realizado por	El equipo de análisis

Resultado 4.3-23 Definir criterio de probabilidad

Fuente: Los autores

4.3.2.4.4.3 Observaciones

Debido a la falta de datos históricos, se encontró que los criterios subjetivos asociados a cada participante tuvieron mucho peso.

4.3.2.4.4.4 Recomendaciones

Se recomienda refinar la lista de participantes en los talleres en que se incorpora la probabilidad en el análisis de riesgo, debido a que la subjetividad inherente a

las elecciones de cada participante proporciona un gran aporte, por tanto estos participantes deben ser personas de mucha experiencia y conocimiento del negocio.

4.3.2.4.5 Actividad 22: Valorar la probabilidad de incidente

4.3.2.4.5.1 Detalle de ejecución

El equipo de análisis, a través de talleres con los participantes, valoró la probabilidad (frecuencia de ocurrencia) para cada una de las ramas con riesgo de los perfiles de riesgo. Para esto, se analizó el riesgo de cada rama, en relación el criterio de probabilidad y la descripción de probabilidad correspondiente al riesgo analizado para el efecto.

4.3.2.4.5.2 Resultado obtenido

Árbol de amenaza basado en activo para Actores humanos utilizando la red

Activo	Acceso	Actor	Motivo	Resultado	Área de Interés	Impacto	Probabilidad
Sieeq Comercial	Red	Interno	Accidental	Revelación			
				Modificación	2, 7	A-M-B	M
				Pérdida		A-M-B	B
				Interrupción		M-B	B
			Deliberado	Revelación	3, 5	A-M-B	M
				Modificación	1, 6	A-M-B	M
				Pérdida	6	A-M-B	B
				Interrupción		M-B	B
		Externo	Accidental	Revelación			
				Modificación			
				Pérdida			
				Interrupción			
			Deliberado	Revelación		A-M-B	B
				Modificación	6	A-M-B	B
				Pérdida	6	A-M-B	B
				Interrupción		M-B	M

Observaciones	
Fecha	17-oct-12
Realizado por	El equipo de análisis

Resultado 4.3-24 Perfil de riesgo con probabilidad e impacto, Sieeq Comercial (acceso red)

Fuente: Los autores

Los perfiles de riesgo con probabilidad e impacto valorados, completos, pueden encontrarse en el Anexo 7.

4.3.2.4.5.3 Observaciones

Las valoraciones de seguridad determinadas dependen en gran medida de la experiencia colectiva de los participantes del taller.

Para el caso de la valoración de probabilidad, no existen rangos, únicamente se presentan valores asociados a la respectiva escala cualitativa determinada en la metodología de estimación de riesgos.

4.3.2.4.5.4 Recomendaciones

Realizar un análisis ordenado por activo y por categoría de amenaza, de esta manera se facilita la valoración de probabilidades al mantener un mismo contexto por activo.

4.3.2.4.6 Actividad 23: Estimar (valorar) y priorizar el nivel de riesgo

4.3.2.4.6.1 Detalle de ejecución

El equipo de análisis, a través de talleres con los participantes, estimó el nivel de riesgo en base a aplicar la metodología de estimación de riesgos para cada una de las combinaciones de valoración de impacto y probabilidad que se establecieron en los perfiles de riesgo. Para los casos en que la valoración de impacto estaba asociada a un rango como por ejemplo A-M-B, se aplicó la metodología de igual forma que si hubiese sido un valor simple, obteniendo como resultado, por ejemplo para una probabilidad alta, un riesgo estimado de A-M.

Posteriormente, para cada riesgo estimado, se definió el valor de priorización en base al análisis del riesgo con el criterio de evaluación de riesgo. Al ser esta la primera implementación del modelo de gestión de riesgos de seguridad de la información en la EEQ, y debido a que todos los activos críticos están asociados al proceso de facturación, que corresponde al macro-proceso de comercialización, se encontró que los valores de priorización de todos los riesgos fueron los mismos, y correspondían a “A,B,B”, que corresponde a una prioridad alta para el valor estratégico de los procesos de negocio, una valoración baja para requisitos legales y contractuales; y una valoración baja para los requisitos y expectativas de los interesados. Debido a que el criterio de evaluación de riesgos no aportó en la priorización, fue necesario acudir al riesgo estimado para realzar la priorización.

4.3.2.4.6.2 Resultado obtenido

Árbol de amenaza basado en activo para Actores humanos utilizando la red									
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Área de Interés**	**Impacto**	**Probabilidad**	**Riesgo estimado**	**Prioridad**
Sieeq Comercial	Red	Interno	Accidental	Revelación					
				Modificación	2, 7	A-M-B	M	A-M-B	A,B,B
				Pérdida		A-M-B	B	M-B	A,B,B
				Interrupción		M-B	B	B	A,B,B
			Deliberado	Revelación	3, 5	A-M-B	M	A-M-B	A,B,B
				Modificación	1, 6	A-M-B	M	A-M-B	A,B,B
				Pérdida	6	A-M-B	B	M-B	A,B,B
				Interrupción		M-B	B	B	A,B,B
		Externo	Accidental	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
			Deliberado	Revelación		A-M-B	B	M-B	A,B,B
				Modificación	6	A-M-B	B	M-B	A,B,B
				Pérdida	6	A-M-B	B	M-B	A,B,B
				Interrupción		M-B	M	M-B	A,B,B
Observaciones									
Fecha	22-oct-12								
Realizado por	El equipo de análisis								

Resultado 4.3-25 Perfil de riesgo con riesgo estimado y prioridad, Sieeq Comercial (acceso red)

Fuente: Los autores

Los perfiles de riesgo con el nivel de riesgo estimado, completos, pueden encontrarse en el Anexo 7.

A continuación se muestra la lista de riesgos altos agrupados por su prioridad:

Riesgos Altos								
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Área de Interés**	**Impacto**	**Probabilidad**	**Riesgo estimado**
Sieeq Comercial	Red	Interno	Accidental	Modificación	2,7	A-M-B	M	A-M-B
Sieeq Comercial	Red	Interno	Deliberado	Revelación	3, 5	A-M-B	M	A-M-B
Sieeq Comercial	Red	Interno	Deliberado	Modificación	1, 6	A-M-B	M	A-M-B
Sieeq Comercial	Fisico	Interno	Accidental	Modificación		A-M-B	M	A-M-B
Sieeq Comercial	Fisico	Interno	Deliberado	Revelación	4	A-M-B	M	A-M-B
Sieeq Comercial	Fisico	Interno	Deliberado	Modificación		A-M-B	M	A-M-B
Sieeq Comercial	-	Defectos de SW	-	Interrupción	9, 10	M-B	A	A-M
Sieeq Comercial	-	Problemas o indisponibilidad de comunicaciones	-	Interrupción	12	M-B	A	A-M
Personal de tratamiento de facturación	-	Falta de capacitación del personal alterno	-	Interrupción	15	M-B	A	A-M
Datamart	Red	Interno	Deliberado	Revelación	15	A-M-B	M	A-M-B

Resultado 4.3-26 Riesgos altos

Fuente: Los autores

La lista de riesgos medios y bajos puede encontrarse en el Anexo 7.

4.3.2.4.6.3 Observaciones

Debido a que todos los riesgos tienen el mismo valor de prioridad, fue necesario priorizar los riesgos únicamente con la ayuda del riesgo estimado.

4.3.2.4.6.4 Recomendaciones

Se recomienda organizar los riesgos en cuadro, ordenándolos de mayor a menor, con el objetivo de tener la lista de riesgos priorizados.

4.3.2.5 Proceso de tratamiento al riesgo

4.3.2.5.1 *Actividad 24: Crear una estrategia de protección*

4.3.2.5.1.1 Detalle de ejecución

El equipo de análisis realizó una revisión de los controles existentes e inexistentes sobre los dominios de la norma ISO/IEC 27002:2005 con el objetivo de definir estrategias que permitan mejorar o corregir la manera en que la EEQ está aplicando o dejando de aplicar los mencionados los controles. Para lograr este objetivo, el equipo de análisis revisó cada uno de los 133 controles asociados a los 11 dominios, determinando las recomendaciones de mejora para cada control. Posteriormente, el equipo de análisis realizó un refinamiento de estas estrategias con personal de planificación estratégica.

Para facilitar la generación de las estrategias, se utilizó como referencia las respuestas a las preguntas clave por cada dominio, que incluye encontrar que se puede mejorar, que se está haciendo mal, que se está haciendo bien y debe continuar utilizándose y las posibles nuevas estrategias a adoptar.

Considerando los resultados del análisis de cumplimiento de controles sobre la norma ISO/IEC 27002:2005 que se había realizado en la actividad 14, donde se concluye que no se cumple con los controles de la gran mayoría de dominios; se consideró necesario realizar un resumen de las estrategias, focalizándolas al largo plazo.

4.3.2.5.1.2 Resultado obtenido

Resultados de definición de estrategia de protección			
Controles de la norma ISO/IEC 27002:2008			
Ítem	Sección	Preguntas Clave	Estrategias
A.5	**Política de Seguridad**	Que se puede hacer para mejorar? Que se está haciendo mal? Prácticas actuales que se deben continuar utilizando? Nuevas estrategias a adoptar?	Redactar, aprobar y comunicar a la brevedad una política de Seguridad de Información. Desarrollar un procedimiento de revisión de la política de seguridad incluyendo cronograma y período de revisión.
A.6	**Aspectos organizativos de seguridad de la información**	Que se puede hacer para mejorar? Que se está haciendo mal? Prácticas actuales que se deben continuar utilizando? Nuevas estrategias a adoptar?	Identificar las necesidades de soporte de especialistas en seguridad de la información. Involucrar en la coordinación de la seguridad de la información la colaboración de los gerentes, usuarios, administradores, diseñadores de aplicación, auditores, personal de seguridad, y especialistas especializados en áreas de seguros, temas legales, recursos humanos, TI y gestión del riesgo. Asignar las responsabilidades de la seguridad de la información en concordancia con la política de seguridad de la información. Definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos. Definir la metodología para la autorización de servicios de procesamiento de la información. Definir acuerdos de confidencialidad para que los empleados los firmen como parte de sus términos y condiciones iniciales de empleo. Establecer procedimientos que especifiquen bajo que condiciones y a que autoridades se debe contactar cuando un incidente de seguridad de información ha sido identificado. Establecer acuerdos de intercambio de información para mejorar la cooperación y coordinación de temas de seguridad. Promover la revisión independiente impulsada por la gerencia. Establecer análisis de los entornos de terceros que manejan información de la EEQ.
A.7	**Gestión de activos**	Que se puede hacer para mejorar? Que se está haciendo mal? Prácticas actuales que se deben continuar utilizando? Nuevas estrategias a adoptar?	Inventariar todos los activos y documentar la importancia de estos activos. Propiciar que todos los empleados, contratistas y terceros, usuarios de los activos que manejen información deben obedecer las reglas de uso aceptable. Establecer un criterio de clasificación de la información, y un proceso formal de clasificación. Clasificar todos los activos de información existentes utilizando estos criterios y procedimientos específicos. Etiquetar los activos reflejando la clasificación de acuerdo a las reglas establecidas.

Resultado 4.3-27 Definición de estrategia de protección

Fuente: Los autores

La estrategia de protección completa, puede encontrarse en el Anexo 7.

4.3.2.5.1.3 Observaciones

Se encontró que hay una gran cantidad de controles que no se cumplen en EEQ, por lo que hay también muchas oportunidades de mejoramiento.

4.3.2.5.1.4 Recomendaciones

Cuando hay una gran cantidad de controles que no se cumplen, se genera también una gran cantidad de estrategias, que se recomienda sean resumidas y refinadas con personal de planificación estratégica, con el objetivo de obtener un conjunto de estrategias consolidado y conciso.

4.3.2.5.2 Actividad 25: Crear planes de mitigación

4.3.2.5.2.1 Detalle de ejecución

El equipo de análisis realizó una revisión de todos los perfiles de riesgo de los cinco activos críticos elegidos para la EEQ, para cada una de las ramas de los árboles que indican de ellos se comparó el riesgo estimado con el criterio de

aceptación del riesgo, de esta forma se obtuvo el enfoque de tratamiento, que indica si el riesgo se reduce, retiene, transfiere o evita.

Posteriormente, se definió por cada árbol de amenaza los planes de mitigación y acciones específicas que permiten aplicar el enfoque de tratamiento al contexto global de todos los riesgos involucrados en el árbol de amenaza revisado. Esto se realiza de este modo pues cada árbol de amenaza está asociado a un mismo activo y a una misma categoría de amenaza, por tanto los planes y acciones definidas aplican a todos los riesgos presentes en el árbol.

Una vez que se definió los planes de tratamiento con sus correspondientes acciones, se realizó una iteración sobre el proceso de evaluación del riesgo, donde se valoró nuevamente el impacto y la probabilidad, pero considerando la aplicación hipotética de los mencionados planes y acciones. Estos nuevos valores de probabilidad e impacto generan también un nuevo riesgo estimado; todos estos valores se apuntan en el perfil de riesgo analizado. Posteriormente, este nuevo riesgo estimado se comparó nuevamente con el criterio de aceptación del riesgo, se encontró que ninguno de los nuevos riesgos estimados incumplió el criterio de aceptación, de este modo no se obtuvo riesgo residual.

Posteriormente, se realizó una revisión de todos los planes de mitigación a través de todos los perfiles de riesgo, se encontró que muchos de los planes que se repetían en varios perfiles de riesgos sobre varios activos, a estos planes se los marcó como prioritarios.

Adicionalmente, se observó que los riesgos asociados a eventos catastróficos debían asociarse a la planificación de continuidad de negocio y de recuperación de datos de la EEQ.

Finalmente, todos los planes de tratamiento y acciones generadas se revisaron con el personal de planificación estratégica en busca de realizar un primer acercamiento para encaminar la planificación de estos planes en asociación a la Dirección de tecnología de la información y comunicaciones.

4.3.2.5.2.2 Resultado obtenido

Árbol de amenaza basado en activo para Actores humanos utilizando la red									
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Impacto**	**Probabilidad**	**Riesgo estimado**	**Enfoque de tratamiento**	**Plan de mitigación, acciones específicas**
Sieeq Comercial	Red	Interno	Accidental	Revelación					-Capacitar a los usuarios sobre la parametrización de facturación y pliegos tarifarios. * Capacitar a los usuarios en manejo de respaldos de reportes importantes. * Implementar un esquema de auditoría y firewall de base de datos. * Restringir la reportería de información sin filtros. * Promover a los usuarios el comprender la importancia de mantener la confidencialidad e integridad de la información de los clientes y sus facturas. - Fortalecer la autenticación del Sieeq Comercial a un esquema de contraseñas más complejo. * Promover el reporte de incidentes de seguridad por parte de los usuarios. **Acciones:** - Empezar a registrar los incidentes de seguridad del Sieeq Comercial. - Realizar pruebas de acceso de escritura a los ejecutables del Sieeq Comercial. - Desinstalar todo cliente o utilitario de acceso a base de datos de los equipos de los usuarios.
				Modificación	A-M-B a M-B	M a B	A-M-B a B	Reducir	
				Pérdida	A-M-B a M-B	B	M-B a B	Reducir	
				Interrupción	M-B	B	B	Retener	
			Deliberado	Revelación	A-M-B a M-B	B	A-M-B a B	Reducir	
				Modificación	A-M-B a M-B	M a B	A-M-B a B	Reducir	
				Pérdida	A-M-B a M-B	B	M-B a B	Reducir	
				Interrupción	M-B	B	B	Retener	
		Externo	Accidental	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
			Deliberado	Revelación	A-M-B a M-B	B	M-B a B	Reducir	
				Modificación	A-M-B a M-B	B	M-B a B	Reducir	
				Pérdida	A-M-B a M-B	B	M-B a B	Reducir	
				Interrupción	M-B a B	M a B	M-B a B	Reducir	
Observaciones	No existe riesgo residual, mediante la aplicación de los planes el riesgo estimado se reducen todos los riesgos al nivel bajo.								
Fecha	05-nov-12								
Realizado por	El equipo de análisis								

Resultado 4.3-28 Perfil de riesgo con planes de mitigación y acciones, Sieeq Comercial (acceso red)

Fuente: Los autores

Los perfiles de riesgo con los planes de mitigación y acciones definidas, completos, pueden encontrarse en el Anexo 7.

4.3.2.5.2.3 Observaciones

La re evaluación de los riesgos no ha generado riesgos residuales, por tanto no fue necesaria otra iteración sobre esta evaluación y tampoco se requerirá la aprobación de riesgos residuales.

4.3.2.5.2.4 Recomendaciones

Se recomienda realizar un análisis de los planes de mitigación en relación a los planes anuales de contrataciones, con el objetivo de verificar aquellos casos que ya cuentan con presupuesto para su ejecución.

4.3.2.5.3 Actividad 26: Crear lista de acciones

4.3.2.5.3.1 Detalle de ejecución

El equipo de análisis revisó todas las acciones que apoyan la implementación de los planes de mitigación definidas en la actividad anterior, con el objetivo de detectar aquellos casos en que la acción podía ser implementada en el corto plazo, sin necesidad de capacitación específica. Se detectó que todas las acciones cumplían con este requisito, de acuerdo a esto, se les agrupó por responsable de ejecución, definiendo adicionalmente la fecha estimada de cumplimiento y las acciones de gestión requeridas.

Debido a que estas acciones ya fueron revisadas con el personal de planificación estratégica en la actividad anterior, no fue necesario realizar esta revisión nuevamente.

4.3.2.5.3.2 Resultado obtenido

Resultado de crear lista de acciones			
Lista de acciones			
No.	**Acción**	**Información**	
1	- Empezar a registrar los incidentes de seguridad del Sieeq Comercial. - Realizar pruebas de acceso de escritura a los ejecutables del Sieeq Comercial. - Desinstalar todo cliente o utilitario de acceso a base de datos de los equipos de los usuarios. - Empezar a registrar los incidentes de seguridad del Datamart. - Empezar a registrar los incidentes de seguridad del Sistema móvil de lecturas. - Empezar a registrar los incidentes de seguridad del Sidebench. - Realizar pruebas de acceso de escritura a los ejecutables del Sidebench.	**Responsable**	Sección de Help Desk
		Fecha de cumplimiento	En los próximos 30 días
		Acciones de gestión requeridas	Previo al registro de incidentes de seguridad, es necesario promover el reporte de estos incidentes por parte de los usuarios.
2	- Activar los protectores de pantalla con contraseña. - Actualizar los procedimientos de subida de todos los servicios tecnológicos asociados al Sieeq Comercial. - Actualizar los procedimientos de subida de todos los servicios tecnológicos del Datamart. - Verificar los logs de ejecuciones y tiempos de ejecución de los procesos de carga de datos. - Actualizar los procedimientos de subida de todos los servicios tecnológicos asociados al Sidebench	**Responsable**	Departamento de Data-Center
		Fecha de cumplimiento	En los próximos 30 días
		Acciones de gestión requeridas	Ninguna.

Resultado 4.3-29 Crear acciones

Fuente: Los autores

El resto de acciones, se pueden encontrar en el Anexo 7.

4.3.2.5.3.3 Observaciones

Se encontró que la mayoría de las acciones tenían como responsable a áreas correspondientes a la Dirección de tecnología de la información y comunicaciones.

4.3.2.5.3.4 Recomendaciones

Se recomienda agrupar las acciones por responsable, enfocándose en categorías como cambios en el SW, help desk, servidores y data-center, servicios generales, recursos humanos, etc.

4.3.2.5.4 Actividad 27: Preparar la presentación del tratamiento al riesgo

4.3.2.5.4.1 Detalle de ejecución

El equipo de análisis consideró las secciones de activos, prácticas de seguridad, riesgos identificados, estrategia de protección, planes de mitigación, acciones y riesgo residual; con el objetivo de generar un resumen claro y conciso que sea la base de una presentación para la alta gerencia, en base a esta información estos entes decidirán la aprobación del enfoque de tratamiento.

4.3.2.5.4.2 Resultado obtenido

Resultado de crear presentación de tratamiento del riesgo	
Puntos clave de la presentación	
Punto	**Descripción**
Información de activos.	- Sieeq Comercial.- Este sistema permite aplicar los pliegos tarifarios, procesar desviaciones de lecturas, calcular valores de los conceptos a facturar, determinar montos elevados, generar movimientos contables, generar las facturas, realizar refacturaciones. - Personal de configuración de pliego tarifario.- Este personal tiene el conocimiento de cómo aplicar las regulaciones y nuevas normativas del CONELEC para los cálculos de los consumos, a través de la configuración de los pliegos tarifarios. - Datamart.- Este sistema da apoyo a la toma de decisiones acerca del proceso de facturación. - Sistema móvil de lecturas.- Este sistema permite a los lectores reportar las lecturas obtenidas en trabajo en el campo.
Prácticas de seguridad actuales.	- No se pudo evidenciar la existencia de una política de seguridad de información que se encuentre aprobada y difundida. - No se pudo evidenciar la existencia de un inventario de activos de información ni un procedimiento de clasificación y asignación de dueños de datos, tampoco se cuenta con una metodología para realizar un análisis de riesgos y poder realizar un tratamiento de los riesgos. - Existe poca documentación de Normas, Estándares, Instructivos de Seguridad, Procedimientos Operativos Diarios, que han sido desarrollados, aprobados y difundidos al interior de la EEQ.
	Riesgos altos: - Accesos internos por red o por vía física, accidentales o deliberados que causan modificaciones al Sieeq Comercial.

Resultado 4.3-30 Presentación de tratamiento del riesgo

Fuente: Los autores

La presentación de tratamiento del riesgo puede encontrarse en el Anexo 7.

4.3.2.5.4.3 Observaciones

Se incluyó únicamente los riesgos altos, medios y los planes de mitigación prioritarios, con el objetivo de darle un enfoque crítico a la presentación.

La alta directiva, solicitó la presentación de los documentos de inicialización de los proyectos asociados a la estrategia de protección y planes de mitigación prioritarios, previo a incluirlos en el plan anual de contratación.

4.3.2.5.4.4 Recomendaciones

Se recomienda redactar los enfoques de riesgo y planes de mitigación evitando palabras técnicas desconocidas, de tal forma que sea comprensible la presentación para la alta directiva. Adicionalmente se recomienda realizar de forma previa una revisión de la presentación con el comité de seguridad.

4.3.2.5.5 Actividad 28: Crear los siguientes pasos

4.3.2.5.5.1 Detalle de ejecución

El equipo de análisis en coordinación con el comité de seguridad de la información, solicitó el apoyo de la alta directiva para la puesta en marcha de los planes de mitigación, definiendo lineamientos de gestión que estén enfocados a apalancar la ejecución de los proyectos asociados a la estrategia de protección y planes de mitigación.

4.3.2.5.5.2 Resultado obtenido

Resultado de crear los siguientes pasos	
Acciones de apoyo a la puesta en marcha del tratamiento al riesgo	
- El comité de seguridad de la información trabajará en una propuesta para independizar a la organización para la gestión de riesgos de seguridad de la información de la Dirección de tecnología de la información y comunicaciones. - El comité de calidad asociado a la norma ISO/IEC 9001 trabajará de forma coordinada con el comité de seguridad de la información, con el propósito de alinear sus objetivos. - La gerencia de planificación en conjunto con la áreas involucradas establecerá la planificación de puesta en marcha de la estrategia de protección y planes de mitigación. - La gerencia de planificación en conjunto con la Dirección de tecnología de información y comunicaciones realizarán la documentación de inicicialización de los proyectos asociados a la estrategia de protección y planes de mitigación previos a su inclusión en el plan anual de contrataciones. - La gerencia de planificación y la gerencia comercial, realizarán el seguimiento y apalancamiento de la implementación de la lista de	
Observaciones	
Fecha	26-nov-12
Realizado por	El equipo de análisis

Resultado 4.3-31 Crear los siguientes pasos

Fuente: Los autores

4.3.2.5.5.3 Observaciones

Los proyectos asociados generados en base a la estrategia de protección y planes de mitigación previos a ser aprobados e incluidos en el plan anual de contrataciones, deben presentar la documentación formal de inicialización del proyecto, esta documentación incluye análisis costo-beneficio. Esta documentación está actualmente elaborándose.

4.3.2.5.5.4 Recomendaciones

Se recomienda revisar aquellos proyectos generados en base a la estrategia de protección y planes de mitigación que ya se incluyen en el plan anual de contrataciones, con el objetivo de agilitar su implementación, pues contaría ya con presupuesto.

4.3.2.6 Proceso de comunicación del riesgo

4.3.2.6.1 Actividad 29: Comunicar el riesgo

4.3.2.6.1.1 Detalle de ejecución

El comité de seguridad revisó las estrategias planteadas por el equipo de análisis, estas estrategias le permitirían a la EEQ comunicar los riesgos entre los entes

involucrados, con el propósito de alcanzar un enfoque común de gestión de riesgos. Para esto, se definió lineamientos asociados a planificar reuniones entre la Alta directiva, Comité de seguridad, Directorio, Organización para la gestión de riesgos de seguridad de la información y Dirección de tecnología de la información y comunicaciones; donde se realice la retroalimentación de la temática de riesgos organizacional.

4.3.2.6.1.2 Resultado obtenido

Resultados de comunicación del riesgo	
Plan de comunicación del riesgo	
Objetivos	- Asegurar los resultados de la gestión de riesgos. - Recabar información de riesgos. - Compartir resultados de la evaluación de riesgos y planes de tratamiento. - Evitar o reducir la probabilidad e impacto de las brechas de seguridad de la información debido a la falta de entendimiento entre quienes toman las decisiones y los interesados. - Dar soporte a la toma de decisiones. - Obtener nueva información acerca de seguridad. - Coordinar con otras instancias y planificar respuestas para reducir las consecuencias a incidentes. - Dar sentido de responsabilidad acerca de riesgos a quienes toman decisiones y a los interesados. - Mejorar la concientización frente a los riesgos.
A quien va dirigido	Comité de seguridad de la información, alta directiva, interesados (actores de EEQ), organización de gestión de seguridad de la información, Dirección de tecnología de información y comunicaciones, equipo de análisis.
Estrategias	- Gestionar la inclusión en la agenda de reuniones del directorio de la EEQ un punto relacionado a la retroalimentación acerca de la temática de riesgos de seguridad de la información. Será el delegado del comité de seguridad de la información quien prepare y presente la información necesaria para análisis del directorio. - Planificar y ejecutar talleres de trabajo al menos una vez al mes entre el equipo de trabajo y el comité de seguridad de la información, con el objetivo de retroalimentar información acerca de la temática de riesgos de seguridad de la información en la EEQ. - Planificar y ejecutar reuniones de trabajo al menos una vez al mes entre el comité de seguridad de la información y el comité de calidad, con el objetivo de retroalimentar ambos enfoques.

Resultado 4.3-32 Plan de comunicación

Fuente: Los autores

El plan de comunicación completo puede encontrarse en el Anexo 7.

4.3.2.6.1.3 Observaciones

El rol del comité de seguridad, de ser el enlace entre el equipo de análisis y la alta dirección, apalanca la comunicación continua en el ámbito de riesgos de seguridad de la información.

4.3.2.6.1.4 Recomendaciones

Se recomienda utilizar un esquema documental con el objetivo de registrar la información generada como parte de la comunicación de riesgos este los entes involucrados y así tenerla disponible eficazmente.

4.3.2.7 Proceso de monitoreo y revisión del riesgo

4.3.2.7.1 Actividad 30: Monitorear y revisar los factores de riesgo

4.3.2.7.1.1 Detalle de ejecución

El equipo comité de seguridad de la información, desde que fue nombrado, en coordinación con el equipo de análisis, se encargó de la tarea de monitorear los factores de riesgo como nuevos activos a incluir en el alcance, cambios de los objetivos estratégicos de la EEQ, nuevas vulnerabilidades, incrementos de la probabilidad e impacto de los riesgos e incidentes relevantes de seguridad de la información.

4.3.2.7.1.2 Resultado obtenido

El comité de seguridad no ha registrado un cambio relevante en el monitoreo realizado en los últimos 6 meses.

4.3.2.7.1.3 Observaciones

Debido a que esta es la primera iteración sobre la implementación del modelo de gestión de riesgos de seguridad de la información, y debido a que esta implementación se ha realizado sobre un proceso de un macro procesos de la cadena de valor, a modo de plan piloto; el comité de seguridad de la información no ha encontrado cambios considerables de los factores de riesgo.

4.3.2.7.1.4 Recomendaciones

Se recomienda que el oficial de seguridad de la información recuerde e incluya en los puntos a tratar en cada sesión del comité de seguridad de la información, la revisión de los cambios en los factores de riesgo.

4.3.2.7.2 Actividad 31: Monitorear, revisar y mejorar la gestión de riesgo

4.3.2.7.2.1 Detalle de ejecución

El equipo comité de seguridad de la información, desde que fue nombrado, en coordinación con el equipo de análisis, se encargó de la tarea de monitorear los contextos legal, ambiental, competencia, valoración de riesgo, activos, criterio básico de impacto, criterio de evaluación de riesgo, criterio de aceptación de riesgo, costo total de propiedad y recursos; con el objetivo de mejorar la gestión de riesgos de seguridad de la información.

4.3.2.7.2.2 Resultado obtenido

El comité de seguridad no ha registrado un cambio relevante en el monitoreo y revisión de la gestión de riesgos de seguridad de la información.

4.3.2.7.2.3 Observaciones

Debido a que esta es la primera iteración sobre la implementación del modelo de gestión de riesgos de seguridad de la información, y debido a que esta implementación se ha realizado sobre un proceso de un macro proceso de la cadena de valor, a modo de plan piloto; el comité de seguridad de la información no ha encontrado cambios considerables de los contextos que afectan a la gestión de riesgos de seguridad de la información. Sin embargo si se realizó cambios sobre los criterios de evaluación de riesgos, impacto y aceptación del riesgo de forma previa a su aprobación; estos cambios no se incluyen en el reporte de esta actividad ya que son iteraciones naturales del modelo propuesto.

4.3.2.7.2.4 Recomendaciones

Se recomienda que el oficial de seguridad de la información recuerde e incluya en los puntos a tratar en cada sesión del comité de seguridad de la información, la revisión de los contextos que afectan a la gestión de riesgos de seguridad de la información.

4.4 ANÁLISIS DE RESULTADOS

4.4.1 ASPECTOS GENERALES

El modelo de gestión de riesgos de seguridad de la información propuesto, ha sido aplicado en un caso de estudio específico, el mismo que se detalla en el capítulo anterior. Cada una de las actividades del modelo ha generado resultados que se analizan en este capítulo, sobre la base de la comparación del resultado obtenido con el esperado.

Adicionalmente, se realizará un análisis de aplicabilidad de los enfoques técnico, económico, legal, operacional y de cronograma. Para el efecto del análisis de aplicabilidad técnica del modelo, se emplea el enfoque para determinación de una efectiva evaluación del riesgo proporcionado por The Open Group. Este enfoque es muy útil, debido a que la evaluación de riesgos es uno de los procesos más importantes y comprende gran parte de las actividades del modelo de gestión de riesgos de seguridad de la información propuesto.

4.4.2 ANÁLISIS DE RESULTADOS POR ACTIVIDAD

A continuación se encuentra un análisis de resultados por cada actividad del modelo, donde se muestra el resultado esperado por actividad en contraste con el resultado obtenido.

Como se puede observar en la tabla siguiente, únicamente 2 de las 31 actividades de todo el modelo obtuvieron un resultado parcial acorde al esperado, estas actividades representan el 6% de las actividades de todo el modelo. Por lo que se concluye que el 94% del modelo obtuvo los resultados esperados. Cabe indicar que estas dos actividades que se refieren a la selección y evaluación de vulnerabilidades tecnológicas se han considerado como un proyecto independiente que se está ejecutando con el apoyo de expertos externos especialistas en test de intrusión, actualmente el proyecto está en la fase de contratación. Con el objetivo de asegurar que este proyecto apoye al modelo de gestión de riesgos de seguridad de la información, se ha incluido dentro del alcance la identificación y evaluación de los componentes tecnológicos asociados a los activos críticos detectados en la implementación del modelo.

Actividad	Resultado esperado	Resultado obtenido	El resultado es el esperado? Si/No/Parcialmente
1. Preparación	Coordinador, personal de logística y documentación seleccionados	Coordinador, personal de logística y documentación seleccionados	Si
2. Obtener patrocinio de la alta dirección	Patrocinio de la alta dirección	Patrocinio de la alta dirección	Si
3. Seleccionar a los miembros del equipo de análisis	Equipo de análisis conformado	Equipo de análisis conformado	Si
4. Definir el alcance	Alcance definido	Alcance definido	Si
5. Selección de los participantes	Participantes seleccionados	Participantes seleccionados	Si
6. Determinar la metodología de estimación de riesgo	Metodología de estimación de riesgo definida	Metodología de estimación de riesgo definida	Si
7. Definir el criterio básico de evaluación de riesgo	Criterio básico de evaluación del riesgo definido	Criterio básico de evaluación del riesgo definido	Si
8. Definir el criterio básico de impacto	Criterio básico de impacto definido	Criterio básico de impacto definido	Si
9. Definir el criterio básico de aceptación de riesgo	Criterio básico de aceptación del riesgo definido	Criterio básico de aceptación del riesgo definido	Si
10. Definir la organización para la gestión de riesgos de seguridad de la información	Organización para la gestión de riesgos de seguridad de la información definida	Organización para la gestión de riesgos de seguridad de la información definida	Si
11. Identificar activos	Activos identificados	Activos identificados	Si
12. Identificar las áreas de interés	Áreas de interés identificadas	Áreas de interés identificadas	Si
13. Identificar los requisitos de seguridad	Requisitos de seguridad identificados	Requisitos de seguridad identificados	Si
14. Identificar controles existentes	Controles existentes identificados	Controles existentes identificados	Si
15. Identificar amenazas	Perfiles de amenaza definidos	Perfiles de amenaza definidos	Si
16. Seleccionar los componentes de la infraestructura a evaluar	Componentes de infraestructura a evaluar identificados	La selección de infraestructura tecnológica a ser evaluada forma parte de una consultoría que está siendo contratada, y será ejecutada por expertos en test de intrusión, el avance de este proyecto es de un 20%.	Parcialmente
17. Identificar vulnerabilidades tecnológicas	Listado de vulnerabilidades tecnológicas por activo identificadas	La evaluación de vulnerabilidades tecnológicas forma parte de una consultoría que está siendo contratada, y será ejecutada por expertos en test de intrusión, el avance de este proyecto es de un 20%.	Parcialmente
18. Identificar impacto	Impactos identificados	Impactos identificados	Si
19. Valorar el impacto de las amenazas	Perfiles de riesgo definidos (perfil de amenaza con impacto valorado.	Perfiles de riesgo definidos (perfil de amenaza con impacto valorado.	Si
20. Describir la probabilidad de amenazas	Descripción de probabilidad definida por cada amenaza.	Descripción de probabilidad definida por cada amenaza.	Si
21. Definir el criterio de probabilidad	Criterio de probabilidad definido	Criterio de probabilidad definido	Si
22. Valorar la probabilidad de incidente	Perfiles de riesgo con probabilidad valorada, definidos.	Perfiles de riesgo con probabilidad valorada, definidos.	Si
23. Estimar (valorar) y priorizar el nivel de riesgo	Nivel de estimación del riesgo definido, riesgos priorizados definidos.	Nivel de estimación del riesgo definido, riesgos priorizados definidos.	Si
24. Crear una estrategia de protección	Estrategia de protección definida	Estrategia de protección definida	Si
25. Crear planes de mitigación	Perfiles de riesgo con planes de mitigación, riesgo residual y enfoque del tratamiento, definidos.	Perfiles de riesgo con planes de mitigación, riesgo residual y enfoque del tratamiento, definidos.	Si
26. Crear lista de acciones	Lista de acciones definidas.	Lista de acciones definidas.	Si
27. Preparar la presentación de tratamiento al riesgo	Puntos clave de presentación de tratamiento al riesgo, definidos.	Puntos clave de presentación de tratamiento al riesgo, definidos.	Si
28. Crear los siguientes pasos	Siguientes pasos definidos.	Siguientes pasos definidos.	Si
29. Comunicar el riesgo	Plan de comunicación del riesgo, definido.	Plan de comunicación del riesgo, definido.	Si
30. Monitorear y revisar los factores de riesgo	Plan de monitoreo y revisión, definido.	Plan de monitoreo y revisión, definido.	Si
31. Monitorear, revisar y mejorar de la gestión de riesgo	Monitoreo, revisión y mejora de gestión del riesgo , ejecutado.	Monitoreo, revisión y mejora de gestión del riesgo , ejecutado.	Si

Tabla 4.4-1 Análisis de resultados

Fuente: Los autores

4.4.3 ANÁLISIS DE APLICABILIDAD TÉCNICA

A continuación se detalla el cumplimiento por parte del modelo de gestión de riesgos de seguridad propuesto en relación a los criterios establecidos por The Open Group para una efectiva metodología de evaluación de riesgo.

Proveer de una taxonomía

El modelo de gestión de riesgos de seguridad de la información propuesto provee una taxonomía de riesgo que tiene por objetivo proveer a aquellos que aplican el modelo, del cuerpo de conocimiento que describe el espacio de la problemática de riesgos.

Enfoque probabilístico

El modelo de gestión de riesgos de seguridad de la información propuesto utiliza un enfoque probabilístico basado en la frecuencia de ocurrencia. Adicionalmente provee de un enfoque organizado de cómo definir el criterio de probabilidad y su valoración.

Exactitud

El modelo de gestión de riesgos de seguridad de la información propuesto ha generado resultados exactos acorde a los casos en que ha sido posible obtener información histórica acerca de incidentes de seguridad. Es decir, por ejemplo, un riesgo de probabilidad alta ha sido definido como tal debido a que existe evidencia de incidentes anteriores. Adicionalmente, para apoyar la exactitud de los resultados, se ha enfocado los riesgos considerando la probabilidad y considerando en el análisis toda información objetiva.

Consistente

El modelo de gestión de riesgos de seguridad de la información propuesto tiende por sí mismo a generar resultados repetibles, es decir las conclusiones serían similares, a partir de su implementación por diferentes entes. Para lograr esto, se basa en un conjunto de actividades bien definidas con resultados esperados establecidos.

Defendible

El modelo de gestión de riesgos de seguridad de la información propuesto genera resultados defendibles, pues serán lógicos y verificables con la documentación de resultados generada en cada una de sus actividades.

Lógico

El modelo de gestión de riesgos de seguridad de la información propuesto utiliza un enfoque lógico donde se establece como se afectan sus componentes unos con otros, evitando así las contradicciones.

Enfocado al riesgo

El modelo de gestión de riesgos de seguridad de la información propuesto se enfoca a las métricas importantes de riesgo que son la probabilidad e impacto.

Conciso y útil

El modelo de gestión de riesgos de seguridad de la información propuesto genera resultados para el ente pertinente tanto para su análisis como para la toma de decisiones.

Realizable

El modelo de gestión de riesgos de seguridad de la información propuesto tiende a proveer opciones realizables para quien toma decisiones, basado en el análisis costo-beneficio y priorización de las propuestas de tratamiento.

Incluye planes de acciones

El modelo de gestión de riesgos de seguridad de la información propuesto incluye tres enfoques de tratamiento al riesgo: el enfoque estratégico (largo plazo), el enfoque operativo (mediano plazo) y acciones inmediatas (corto plazo).

Priorizado

El modelo de gestión de riesgos de seguridad de la información propuesto se enfoca en la priorización del tratamiento del riesgo de acuerdo a aplicar los recursos de forma eficiente, enfocándose en los riesgos más altos y en los tratamientos que afectan a varios activos.

Como se puede observar en las descripciones anteriores, el modelo de gestión de riesgos de seguridad de la información propuesto cumple con todos los criterios sugeridos por The Open Group para establecer una efectiva metodología de evaluación de riesgos de seguridad de la información, por tanto y debido a que la evaluación de riesgos forma una gran parte del modelo propuesto y adicionalmente es uno de los más importantes, se puede concluir que el modelo propuesto es también efectivo, por tanto aplicable técnicamente.

4.4.4 ANÁLISIS DE APLICABILIDAD ECONÓMICA

La implementación del modelo de gestión de riesgos de seguridad de la información propuesto ha requerido de la participación de varios funcionarios de la EEQ. A continuación, se muestra un detalle de las horas de participación de cada uno de ellos en conjunto con el costo por hora, con el objetivo de obtener el valor del proyecto en cuanto a recursos de personal.

Personal	Costo por hora	Cantidad de horas	Costo total
Gerencia General	$25,00	14	$350,00
Gerente Distribución	$21,88	14	$306,25
Gerente Subtransmisión	$21,88	14	$306,25
Gerente Planificación	$21,88	14	$306,25
Gerente Comercial	$21,88	150	$3.281,25
Procurador	$21,88	34	$743,75
Auditor	$18,75	14	$262,50
Director de talento humano	$18,75	20	$375,00
Director de TIC	$18,75	98	$1.837,50
Oficial de seguridad	$11,25	198	$2.227,50
Ingeniero de seguridad	$8,75	182	$1.592,50
Ingeniero en Sistemas 1	$8,75	172	$1.505,00
Ingeniero en Sistemas 2	$8,75	96	$840,00
Ingeniero Comercial 1	$8,75	96	$840,00
Ingeniero Comercial 2	$8,75	96	$840,00
Ingeniero Eléctrico 1	$8,75	96	$840,00
Ingeniero Eléctrico 2	$8,75	96	$840,00
Costo total			$17.293,75

Tabla 4.4-2 Costos de personal

Fuente: Transparencia de la información, portal EEQ

Adicional a los costos de personal, a continuación se detalla los costos de equipamiento informático y otros suministros esenciales para la implementación del modelo de gestión de riesgos de seguridad.

Item	Cantidad	Costo por hora	Horas	Costo total
Computador	17	$0,21	1372	$4.898,04
Impresora	1	$0,09	1372	$123,48
Teléfono		$2,40	300	$720,00
Energía Eléctrica		$0,67	1372	$919,24
Papel				$50,00
Internet		$0,03	1372	$45,28
Costo total				$6.756,04

Tabla 4.4-3 Costos de equipos y suministros

Fuente: Reporte de bienes EEQ

Los costos por hora de uso de computador e impresora se obtuvieron dividiendo el valor del equipo para el total de horas útiles (3 años), tomando como referencia un uso semanal de 40 horas.

Para el caso del consumo telefónico, se estimó una utilización de 300 horas durante todo el proyecto, para el caso de la energía eléctrica se consideró el consumo de kw/h de los equipos por el número de horas del proyecto.

Se ha estimado un consumo de $50 en papel. Finalmente, para el consumo de internet se consideró en base a un aproximado de hora de internet por la cantidad de horas del proyecto.

El costo total de la implementación es de $24.049,79. Cabe mencionar que el valor más alto corresponde al pago del personal, sin embargo este valor es cubierto por la EEQ como salario de sus funcionarios aún cuando esta implementación no se hubiese ejecutado.

El análisis económico, asociado al valor actual neto (VAN) y tasa interna de retorno (TIR), considerando todos los proyectos que surjan de las iniciativas de tratamiento del riesgo, no es parte del alcance de este estudio.

4.4.5 ANÁLISIS DE APLICABILIDAD LEGAL

La aplicación del modelo de gestión de riesgos de seguridad de la información propuesto, no ha generado conflictos legales con la ley de comercio electrónico, firmas electrónicas y mensajes de datos, ni con la ley del sistema nacional de registro de datos públicos.

La aplicación del modelo propuesto, tiene por objetivo gestionar los riesgos de seguridad de la información en relación a mantener su confidencialidad, integridad y disponibilidad.

La ley de comercio electrónico, firmas electrónicas y mensajes de datos, regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. De acuerdo a un enfoque de aseguramiento de la confidencialidad, integridad y disponibilidad de la información, el modelo propuesto da soporte a los requisitos legales establecidos en esta ley, especialmente a la sección de los principios generales. A continuación se muestra el detalle de los artículos de la ley que aplican para el efecto y su relación con el modelo propuesto:

- Artículo 5. Confidencialidad y reserva (Confidencialidad).
- Artículo 7. Información original (Integridad).
- Artículo 8. Conservación de los mensajes de datos (Disponibilidad e Integridad).
- Artículo 9. Protección de datos (Confidencialidad).

La ley de registro nacional de datos públicos crea y regula el sistema de registro de datos públicos y su acceso en entidades públicas o privadas que administren estas bases o registros. De acuerdo a un enfoque de aseguramiento de la confidencialidad, integridad y disponibilidad de la información, el modelo propuesto da soporte a los requisitos legales establecidos en esta ley, especialmente a la sección de los principios generales. A continuación se muestra el detalle de los artículos de la ley que aplican para el efecto:

- Artículo 4. Responsabilidad de la información (Las instituciones y personas naturales que administren datos públicos son responsables de la integridad, protección y control de los registros y bases de datos a su cargo).
- Artículo 5. Accesibilidad y confidencialidad (Son confidenciales los datos personales, de intimidad personal, aquellos cuyo uso público atente contra los derechos humanos consagrados en la Constitución, etc.).

Como se puede observar en la descripción anterior, el modelo propuesto al dar soporte a la gestión de riesgos de seguridad de la información, también da

soporte a los artículos de las leyes, en relación a la confidencialidad, disponibilidad e integridad de la información. Adicionalmente, cabe indicar que no va en contra de ninguno de los artículos establecidos en ambas leyes.

Para el caso de estudio, se ha observado la gran utilidad del modelo, especialmente en lo relacionado con el aseguramiento de la confidencialidad de la información sensible de la EEQ, que se relaciona a los datos personales de los clientes, que son regulados por la Ley de registro nacional de datos públicos. Para el efecto, el modelo ha propuesto controles desde varias ópticas, que incluyen la estrategia de protección, los planes de mitigación y la lista de acciones.

4.4.6 ANÁLISIS DE APLICABILIDAD OPERACIONAL

El modelo de gestión de riesgos de seguridad de la información propuesto, es operacionalmente viable, debido a que ha demostrado ser efectivo en sus objetivos, permitiendo resolver la problemática de riesgos de seguridad de la información en la EEQ para el alcance definido para el efecto. Es decir ha permitido identificar, evaluar y proporcionar tratamiento a riesgos de seguridad de la información; esto es verificable en el análisis de resultados realizado en la sección 4.4.2. Adicionalmente, se ha observado que las actividades y su secuencias son las adecuadas, debido a que no han causado conflicto unas con otras. Sin embargo, si se han generado iteraciones sobre algunas de ellas debido a la necesidad de retroalimentación y ajustes propios de la naturaleza no lineal de la gestión de riesgos de seguridad de la información.

Finalmente, cabe indicar que el modelo propuesto cumple con todos los requisitos establecidos para una efectiva evaluación de riesgos de seguridad de la información.

4.4.7 ANÁLISIS DE APLICABILIDAD DE CRONOGRAMA

El modelo de gestión de riesgos de seguridad de la información propuesto, ha sido implementado en algo más de 6 meses, es decir se ha completado de acuerdo a las expectativas establecidas en el diagrama Gantt definido en la actividad de preparación del mencionado modelo (ver Actividad 1 sección 4.3.2.1.1).

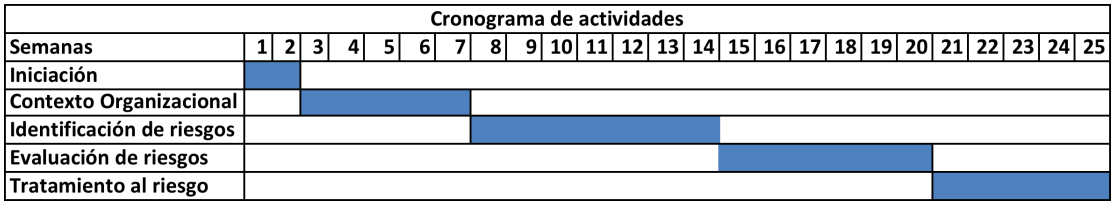


Figura 4.4-1 Diagrama Gantt por procesos

Fuente: Los autores

En la figura anterior, se puede observar el diagrama donde se especifica una cantidad total de 25 semanas equivalente aproximadamente a 6 meses, por lo que se concluye que se ha cumplido con los tiempos previstos. Cabe indicar que el proceso de test de intrusión realizado por expertos, asociado a la identificación y evaluación de vulnerabilidades tecnológicas es un proyecto integral, es decir se refiere a toda la infraestructura tecnológica y no solamente a aquella asociada a los activos críticos, por lo que el tiempo estimado de ejecución es de 12 semanas, que es un considerable incremento de tiempo en relación a las 2 semanas que se había estipulado en el cronograma inicial.

Para cumplir con los cronogramas ha sido necesaria la participación extra por parte de los miembros del área de gestión de riesgos de seguridad de la información, con el objetivo de agilizar el procesamiento y análisis de los datos obtenidos en los talleres. Por tanto, se concluye que el plazos estimado de 6 a 7 meses es razonable para la implementación de un proceso de cadena de valor. Sin embargo, cabe indicar que para posteriores implementaciones del modelo, los tiempos podrían acortarse, debido a que el equipo de análisis cuenta con más experiencia y que algunos de los criterios básicos, metodologías, y enfoques únicamente deberán ser ajustados y no creados sin una referencia inicial.

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La norma ISO/IEC 27005:2008 y el método OCTAVE comprenden un grupo de 11 actividades comunes que en conjunto con 8 actividades propias de la norma ISO/IEC 27005:2008 y 12 actividades propias del método OCTAVE, propician oportunidades de acoplamiento que al ser consolidadas en un esquema integral, logran cumplimentarse unas con otras de tal forma que abarcan las actividades requeridas para la gestión de riesgos de seguridad de la información, que incluye entre otras, a las primordiales que son la identificación y tratamiento del riesgo.
- El afinamiento de las actividades definidas por el esquema de acoplamiento entre la norma ISO/IEC 27005:2008 y el método OCTAVE en un modelo que incluye una taxonomía, terminología, definición detallada de actividades, plantillas y recomendaciones de implementación; cubre una enfoque metodológico completo para la gestión de riesgos de seguridad de la información, que incluye los procesos de iniciación, definición del contexto organizacional, identificación de riesgos, evaluación de riesgos, tratamiento de riesgos, comunicación de riesgos; monitoreo y revisión de riesgos.
- El modelo de gestión de riesgos de seguridad de la información propuesto fue aplicado en un 93% para el caso de estudio práctico, no fue posible la aplicación de dos actividades del modelo debido a que estas fueron consideradas como un proyecto paralelo de test de intrusión manejado por expertos; sin embargo, si es posible asociar estos resultados a los del resto del modelo considerando en el análisis de vulnerabilidades tecnológicas a los componentes tecnológicos asociados a los activos críticos.
- Se validó exitosamente la aplicabilidad técnica del modelo de gestión de riesgos de seguridad de acuerdo a los criterios de los expertos de The Open Group, donde se determinó que el modelo cumple con los requisitos

para una efectiva evaluación de riesgo, que incluye el proveer una taxonomía, enfoque probabilístico, exactitud, consistencia, defendible, lógico, enfocado al riesgo, conciso, útil, realizable, incluye plan de acciones y priorizado.

- Se validó exitosamente la aplicabilidad económica, legal, operacional y de cronograma del modelo de gestión de riesgos de seguridad; encontrando que es viable aplicar el modelo con recursos propios de la EEQ. Además, el modelo cumple con las de leyes y reglamentos, es efectivo en alcanzar sus objetivos y puede ser cumplimentado para un proceso organizacional en un periodo de tiempo de entre 7 y 8 meses con la participación del personal elegido para el efecto y el apoyo de la alta directiva.

A continuación se muestran conclusiones relacionadas a la aplicabilidad operacional del modelo:

- Para una efectiva implementación del modelo de gestión de riesgos de seguridad de la información propuesto se requiere que el equipo de análisis se capacite en la temática de riesgos propuesta en la taxonomía y terminología del modelo, adicionalmente, es primordial el comprometimiento y auspicio de la alta directiva, así como el aseguramiento de la participación activa del personal que conforma los talleres de obtención del conocimiento.
- A partir de la implementación del modelo de gestión de riesgos de seguridad de la información en un segundo proceso de cadena de valor, se reducirán los tiempos en que el equipo de análisis procesa la información obtenida en los talleres, debido a que se cuenta ya con el conocimiento y habilidades para realizar estas actividades.
- Si bien el modelo de gestión de riesgos de seguridad de la información propuesto, provee varios ejemplos con el objetivo de aclarar la temática respecto a la determinación de la metodología de estimación de riesgo, se observó que se requiere aún más información al respecto de otras metodologías, de tal forma que se determine la opción más adecuada para la estimación de riesgo acorde a la propia naturaleza de las organizaciones.

- Se observó que en la selección de los activos críticos realizada en los talleres con los participantes generalmente considera activos relacionados con sistemas de información y personas. De acuerdo a esto, es necesario considerar en el análisis de riesgos los componentes tecnológicos que conforman los sistemas de información, en especial los puntos únicos de falla.
- En el análisis de brechas posterior al mapeo de las áreas de interés en los árboles de amenaza, se detecta riesgos que a primera vista no fueron identificados en la generación de las áreas de interés, por lo que este análisis de brechas es imprescindible con el objetivo de una identificación integral de riesgos por activo.
- El criterio de probabilidad debe establecerse con la mayor cantidad de información objetiva con que se cuente, sin embargo, y dado que en la mayoría de los casos las organizaciones no cuentan con este tipo de información histórica, es necesario cumplimentar el enfoque probabilístico con criterios subjetivos sustentados en la experiencia de los participantes, por lo que es necesario que estos participantes sean grandes conocedores de los procesos de negocio organizacionales.
- En una primera implementación del modelo de gestión de riesgos de seguridad de la información para un proceso de cadena de valor, se observó que la aplicación del criterio de evaluación del riesgo no determinó resultados relevantes, debido principalmente a que este criterio es global para toda la EEQ, por tanto al pertenecer todos los activos a un mismo proceso, los valores de evaluación de riesgo que se utilizan para la priorización del tratamiento al riesgo, resultan iguales. Sin embargo, en posteriores implementaciones sobre otros procesos de la cadena de valor, la aplicación del criterio de evaluación del riesgo si generará resultados concluyentes y útiles para la priorización del tratamiento al riesgo.
- Cuando la aplicación del criterio de evaluación del riesgo no determina resultados concluyentes para la priorización del tratamiento al riesgo, se debe utilizar el nivel de estimación del riesgo para el efecto.
- Se observó que en los riesgos estimados de nivel medio, fue necesario un análisis más profundo con el objetivo de determinar la prioridad del

tratamiento, debido a que algunos de estos riesgos provenían de una probabilidad baja con alto impacto, este tipo de riesgo se asocia generalmente con eventos catastróficos, cuyo tratamiento regularmente aplica a los planes de continuidad de negocio; mientras que los riesgos estimados con valor medio que provienen de una probabilidad alta e impacto bajo, generalmente son mitigados a través de planes y acciones.

- En organizaciones que apenas inician su gestión de riesgos de seguridad de la información, el análisis de cumplimiento de los controles provistos por la norma ISO/IEC 27002:2005 determinan una gran cantidad de incumplimientos, que para el caso de generar la estrategia de protección, deben ser considerados como grandes oportunidad de mejora de la seguridad de la información organizacional.
- Siempre es necesaria al menos una iteración adicional sobre el proceso de evaluación de riesgos cuando se intenta determinar los nuevos valores de probabilidad, impacto y estimación de riesgo, considerando la hipotética aplicación de los planes de mitigación, y lista de acciones.
- Si bien, la priorización de los planes de tratamiento al riesgo debe realizarse en base a una análisis costo-beneficio, es primordial en primeria instancia basar esta priorización en la elección de aquellos planes de tratamiento que apliquen a varios activos, de tal forma que se mitiguen más riesgos.
- En una primera implementación del modelo de gestión de riesgos de seguridad de la información, no se ha observado resultados relevantes del monitoreo y revisión de los factores y gestión del riesgo de seguridad de la información, esto principalmente debido a que en una primera implementación el tiempo transcurrido es corto, sin dar mayor oportunidad a grandes cambios. Sin embargo, en posteriores implementaciones, estos procesos cobran gran importancia debido a que los períodos de implementación se amplían, dando lugar a una mayor posibilidad de ocurrencia de cambios en las organizaciones.
- El comité de riesgos de seguridad de la información es un ente que revisa y discute toda temática de riesgos, sin embargo, no tiene autoridad para aprobar o reprobar políticas, ni criterios de impacto, evaluación o

probabilidad; este tipo de aprobaciones la realiza únicamente la alta directiva

5.2 RECOMENDACIONES

- Si bien el modelo de gestión de riesgos de seguridad de la información propuesto no contempla el seguimiento de la implementación y seguimiento de la estrategia de protección, planes de mitigación y estrategia de mitigación; si se recomienda que se proporcione un enfoque de mejoramiento continuo donde se ha haga seguimiento a las implementaciones de los enfoques de tratamiento al riesgo a través de implementaciones posteriores del modelo propuesto sobre otros procesos de la cadena de valor organizacionales.
- Se recomienda hacer continuas revisiones a través de la ejecución de las actividades del modelo de gestión de riesgos de seguridad de la información, con el objetivo de encontrar posibles brechas y resolver inconsistencias respecto a los resultados obtenidos.
- En el caso de no contar con la suficiente experiencia para realizar un test de intrusión con el propósito de evaluar las vulnerabilidades tecnológicas de componentes de infraestructura, se recomienda considerar la opción de contactar con expertos el ethical hacking para realizar estas actividades.
- Se recomienda utilizar herramientas de manejo de documentación y manejo de proyectos con el objetivo de facilitar la gestión de los resultados y cronogramas asociados a la implementación de las actividades del modelo de gestión de riesgos de seguridad de la información propuesto.
- Con el objetivo de cumplimentar una gestión integral de seguridad de la información, se recomienda cumplimentar la implementación del modelo de gestión de riesgos de seguridad de la información con auditorías de seguridad, análisis GAP de normas de seguridad y gobierno de seguridad.
- Se recomienda asociar formalmente la gestión del plan de continuidad de negocio organizacional y el plan de recuperación ante desastres con el modelo de gestión de riesgos de seguridad de la información, con el objetivo de realizar una implementación integral de estas iniciativas asociadas en mayor o menor grado a la seguridad de la información.

- En los casos en que las organizaciones cuenten con certificaciones ISO/IEC de calidad, se recomienda integrar el sistema de gestión de la calidad con el modelo de gestión de riesgos de seguridad de la información, a través de formalizar reuniones periódicas entre el comité de seguridad de la información y el comité de la calidad, con el propósito de unificar criterios de gestión de riesgos que sean transversales a toda la organización.
- Se recomienda dar énfasis en la ejecución de los enfoques de tratamiento al riesgo establecidos en la estrategia de protección, planes de mitigación y lista de acciones que están asociados al cumplimiento de las normativas legales tanto de la ley de comercio electrónico, firmas electrónicas y mensajes de datos, como de la ley de registro nacional de datos públicos.

REFERENCIAS BIBLIOGRÁFICAS

1. **Alberts, Christopher y Dorofee, Audrey.** *OCTAVE Method Implementation Guide Version 2.0.* Vol. Volume 14: Bibliography and Glossary.

2. **International Organization for Standardization.** *Information technology – Security techniques – Information security risk management.* Geneva : s.n., 2008. ISO/IEC 27005:2008.

3. **Carnegie Mellon University.** OCTAVE. *OCTAVE Method.* [En línea] 17 de Sepriembre de 2008. http://www.cert.org/octave/octavemethod.html.

4. **Alberts, Christopher y Dorofee, Audrey.** *Managing Information Security Risks - OCTAVE Approach.* Boston : Addison-Wesley, 2002.

5. **British Standards Institution.** *Information Security Management, Part 1: Code of Practice for Information Security Management of Systems.* Londres : s.n., 1995. BS7799.

6. **Swanson, Marine y Guttman, Barbara.** *Generally Accepted Principles and Practices for Securing Information Technology Systems.* Washington D.C : s.n., 1996. NIST SP 800-14.

7. **The Open Group.** The Open Group - Risk Taxonomy. [En línea] Enero de 2009. [Citado el: 1 de Mayo de 2012.] https://www2.opengroup.org/ogsys/publications/viewDocument.html;jsessionid=786C582691A090393A13712FE176562E?publicationid=12156&documentid=10743.

8. **International Organization for Standarization.** *Information technology - Security techniques - Information security management system implementation guidance.* Geneva : s.n., 2010. ISO/IEC 2003:2010.

9. **International Organization for Standardization.** *Information technology - Security techniques - Information security management systems - Requirements.* Geneva : s.n., 2005. ISO/IEC 27001:2005.

10. **The Open Group.** The Open Group - Risk Methodology Requirements. [En línea] Enero de 2009. [Citado el: 1 de Mayo de 2012.] http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf.

ANEXOS

ANEXO 1: NOMENCLATURA PARA COMPARATIVA NORMA ISO/IEC 27005:2008, MÉTODO OCTAVE.

ANEXO 2: DESCRIPCIONES COMPARATIVAS DETALLADAS DE LA NORMA ISO/IEC 27005:2008 Y EL MÉTODO OCTAVE.

ANEXO 3: OPORTUNIDADES DE ACOPLAMIENTO ENTRE LA NORMA ISO/IEC 27005:2008 Y EL MÉTODO OCTAVE.

ANEXO 4: PERFIL GENÉRICO DE RIESGOS.

ANEXO 5: PERFIL GENÉRICO DE RIESGOS PARA EEQ.

ANEXO 6: PLANTILLAS.

ANEXO 7: RESULTADOS.