### Definición de requerimientos funcionales y no funcionales

**4.1.3.1 Requerimientos funcionales:**

* Inicio de sesión de usuarios con sus respectivos roles en el sistema.
* El administrador podrá crear, modificar, mostrar y eliminar usuarios, auditorias, tareas, informes, hallazgos, etc. Cabe destacar que es el único usuario que puede llevar a cabo las 4 acciones.
* El líder solo podrá crear, modificar y mostrar las auditorias y tareas, además de ver la información que los demás auditores suben al sistema.
* El rol de auditor solo podrá realizar las tareas que le sean asignadas por su auditor líder y ver la información que lo demás auditores suben al sistema.
* Si los auditores no están asignados a una auditoria no podrán ver dicha información.
* Gestión de planificación y asignación de actividades de auditoria
* Gestionar procesos de identificación, análisis, evaluación y tratamiento de riesgos
* Generación de graficas pertinentes al sistema
* Generación de reportes pertinentes al sistema

**4.1.3.2 Requerimientos no funcionales**

* La interfaz debe ser agradable y comprensible para el usuario
* El sistema debe ser capaz de operar adecuadamente
* La aplicación debe cumplir con la confidencialidad, disponibilidad e integridad de la información.

**Valoración de los activos**

VA= C+I+D

|  |  |
| --- | --- |
| **Criterio** | **Valor** |
| Muy bajo | 1 |
| Bajo | 2 |
| Medio | 3 |
| Alto | 4 |
| Muy alto | 5 |

**Amenazas**

* Infraestructura: fallos de suministro eléctrico, refrigeración, contaminación, etc.
* Origen natural: inundaciones, terremotos, incendios, rayos, etc.
* Fallos de los sistemas informáticos y de comunicaciones: aplicaciones o equipos de transmisión Caida del servicio, virus, toyanos, falta de mantenimiento
* Error humano: errores accidentales o deliberados de las personas que actúan con la información.

**Impacto**

|  |  |  |  |
| --- | --- | --- | --- |
| **Valor - Criterio** | | **Descripción** | **Pérdida de utilidad operacional** |
| 1 | Insignificante | No genera pérdidas financieras ni compromete de ninguna forma la imagen pública de la institución y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos. | Menor de ½ día |
| 2 | Menor | Puede generar pérdidas financieras que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la institución y del Gobierno. Su materialización causaría un bajo daño en del desarrollo del proceso y no afectaría el cumplimiento de los objetivos. | ½ día o 1 día |
| 3 | Serio | Puede generar pérdidas financieras que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la institución y del Gobierno. Su materialización causaría un deterioro en del desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente de forma normal | De 1 día a una semana |
| 4 | Desastroso | Generación de pérdidas financieras que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la institución y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal. | De una semana a un mes |
| 5 | Catastrófico | Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren. | Más de un mes |

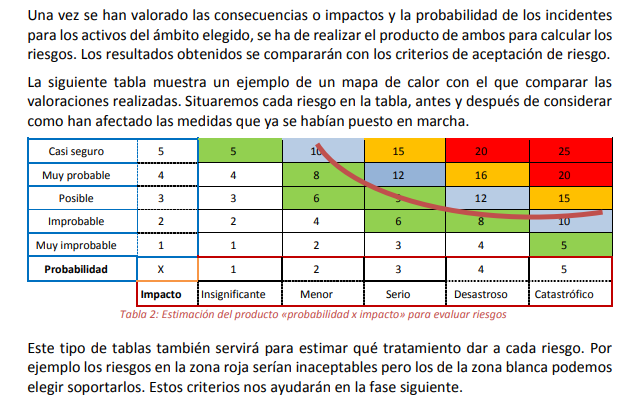
Tabla 1 Criterios de Impacto Fuente: ISO 27001

**Probabilidad de ocurrencia**

|  |  |
| --- | --- |
| **Valor** | **Criterio** |
| 1 | Muy improbable |
| 2 | Improbable |
| 3 | Posible |
| 4 | Muy probable |
| 5 | Casi Seguro |

**Matriz de riesgo según la metodología COSO- ERM gestión de riesgos empresariales**

Riesgo= impacto x probabilidad



**Niveles de riesgos**

Baja: baja exposición y severidad para lo cual se recomienda monitoreo (COLOR VERDE)

Moderado: se recomienda que estos riesgos sean gestionados en niveles básicos de la compañía pero con supervisión directa del responsable (COLOR AMARILLO)

Alta: riesgos que requieren controles y alarma permanente que permitan su gestión constante (COLOR NARANJA)

Extremo: riesgos de alta severidad y exposición para los cuales se deben implementar controles para su adecuado tratamiento, debido a su importancia y criticidad son de máxima prioridad para la compañía. (COLOR ROJO)

|  |
| --- |
| **Nivel de riesgo** |
| Baja |
| Moderado |
| Alta |
| Extremo |

**-Tratamiento del riesgo (caso de no tener controles aplicados) COSO GESTION DE RIESGOS EMPRESARIALES**

Clasificación del control

|  |  |
| --- | --- |
| **Oportunidad de la acción del control** | |
| **Clasificación** | **Descripción** |
| Preventivo | Controles que actúan antes o al inicio de un proceso |
| Correctivo | Controles que actúan durante el proceso y que permiten corregir las deficiencias |
| Detectivo | Controles que actúan una vez que termine el proceso |

|  |  |
| --- | --- |
| **Periodicidad en la acción del control** | |
| **Clasificación** | **Descripción** |
| Permanente | Controles que se aplican durante todo el proceso, es decir en cada operación |
| Periódico | Controles que se aplican en forma constante solo cuando ha transcurrido un periodo especifico de tiempo |
| Ocasional | Controles que se aplican de forma ocasional en un proceso |

|  |  |
| --- | --- |
| **Automatización en la aplicación del control** | |
| **Clasificación** | **Descripción** |
| Automatizado | La aplicación del control es completamente automatizada |
| Semi-automatizado | Parcialmente aplicada mediante sistemas automatizados |
| Manual | No está considerado el uso de sistema automatizados |

**Valoración de la clasificación de los controles**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Frecuencia u oportunidad** | **Tipo de control o Periodicidad** | **Automatización** | **Criterio** | **Valor** |
| Permanente | Preventivo | Automatizado  Manual | Optimo | 3 |
| Permanente | Correctivo | Automatizado  Manual |
| Periódico | Preventivo | Automatizado  Manual | Regular | 2 |
| Periódico | Correctivo | Automatizado  Manual |
| Ocasional | Correctivo | Automatizado  Manual | Deficiente | 1 |
| Ocasional | Preventivo | Automatizado  Manual |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Frecuencia u oportunidad** | **Tipo de control o Periodicidad** | **Automatización** | **Criterio** | **Valor** |
| Permanente | Preventivo | Automatizado  Manual | Optimo | 5 |
| Permanente | Correctivo | Automatizado  Manual |
| Permanente | Detectivo | Automatizado  Manual | Bueno | 4 |
| Periódico | Preventivo | Automatizado  Manual |
| Periódico | Correctivo | Automatizado  Manual | Mas que regular | 3 |
| Periódico | Detectivo | Automatizado  Manual |
| Ocasional | Preventivo | Automatizado  Manual | Regular | 2 |
| Ocasional | Correctivo | Automatizado  Manual |
| Ocasional | Detectivo | Automatizado  Manual | Deficiente | 1 |

**Riesgo residual:** es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometida una compañía nunca puede erradicarse totalmente. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable).

**Riesgo inherente:** es propio del trabajo o proceso, que no puede ser eliminado del sistema; es decir, en todo trabajo o proceso se encontrarán riesgos para las personas o para la ejecución de la actividad en sí misma.

Riesgo inherente – controles = riesgo residual

**Reducción del riesgo y riesgos residual:** en los riesgos que se han decidido tratarse ha reducido el riesgo en una cantidad “X” quedando normalmente un riesgo menor a la inicial, al cual se denomina riesgo residual.

**Evaluación de la madurez** El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. Antes de abordar intentaremos profundizar al máximo en el conocimiento de la organización. De forma resumida, los dominios que se analizaron son:

* Política de seguridad
* Organización de la seguridad de la información.
* Gestión de activos.
* Seguridad en los recursos humanos.
* Seguridad física y ambiental.
* Gestión de comunicaciones y operaciones.
* Control de acceso.
* Adquisición, desarrollo y mantenimiento de sistemas de información.
* Gestión de incidentes
* Gestión de continuidad de negocio
* Cumplimiento

En este estudio se realizó una revisión de los controles planteados por la norma para cumplir con los diferentes objetivos de control. Esta estimación se desarrollo basado en el modelo de madurez de la capacidad (CMM), ver la tabla Nro. 15