ASI- Administración de la seguridad de la información

Documento de resultados del análisis de riesgos. Formato ASI F3

1. OBJETIVO DEL ANÁLISIS DE RIESGOS:

[Se sugiere partir del siguiente enunciado: Elaborar un Reporte final, mediante el cual se informe la lista de controles recomendados, para un adecuado tratamiento de los riesgos detectados en el orden de prioridad previamente establecido, indicando además los requerimientos para su implementación (económicos, materiales y de personal). Se debe incluir en el reporte el nivel de riesgo residual de cada escenario, utilizando el apartado correspondiente del presente formato.]

Lista de controles recomendados

Prioridad *[Establecer en orden de prioridades, cuales controles se recomienda sean implementados]*	Control recomendado *[Por cada control, indicar cuales son las amenazas que enfrentan, y que activos son los que se ven protegidos]*	Amenazas a mitigar	Activos a proteger	Riesgos residuales *[Por cada activo protegido, resumir cual es el riesgo residual que será asumido, explicando la justificación para ello]*	Requerimientos especiales *[Indicar los requerimientos especiales para cada control recomendado]*	Inversión requerida *[Indicar de acuerdo a los estudios costo beneficio, cual es la inversión requerida y cuál es la pérdida que se pretende evitar (I$)]*
					Total: $	

Riesgos aceptados

[Indicar cuáles son los riesgos aceptados y su justificación.]
[Indicar comentarios respecto a apoyos o limitantes ocurridos durante el desarrollo del estudio.]
[Indicar comentarios relativos a la metodología que se aplica en los presentes formatos.]

Secuencia	Amenazas	Activos de información	Riesgos	Observaciones

Firmas y fechas de elaboración, revisión y autorización del análisis

Fecha de Elaboración: *(DD/MM/AAAA)*

Firma	*Firma*	*Firma*
Nombre	*Nombre*	*Nombre*
Cargo	*Cargo*	*Cargo*
Elaboró	**Revisó**	**Aprobó**

2. DIRECTRIZ DE ADMINISTRACIÓN DE RIESGOS:

Objetivo y alcance

[Definir el objetivo y alcance de la directriz que rija sobre el proceso de Administración de la seguridad de la información ASI, deberá expresar la necesidad de contar, en el contexto de la propia Institución, con los mecanismos, elementos, herramientas y todos aquellos apoyos que permitan reaccionar ante un amenaza o vulnerabilidad que se materializa y mitigarlas con los menores daños y costos posibles.]

Justificación

[Describir los elementos internos y externos que obligan al establecimiento de la administración de riesgos, es posible fundamentar en eventos pasados que impactaron a la Institución en sus bienes y servicios, o implementaciones de la administración de riesgos ya efectuadas que han mostrado beneficios significativos.]

Requerimientos regulatorios

[Describir las regulaciones del marco normativo que resulten aplicables a los riesgos identificados.]

Elementos para la administración de riesgos

Elemento	Grupo de riesgos sobre los que incide *[Indicar los riesgos sobre los que incide]*	Escenario *[Definición de cada elemento]*
Umbrales de tolerancia al riesgo		
Mecanismos que se utilizarán para medir la correcta administración de riesgos		
Estrategias de mitigación		
Periodicidad con la que se informará a los involucrados en el proceso		

Directrices de administración de riesgos

Necesidad *[Indicar la necesidad que tiene la Institución]*	Directriz de Administración de riesgos *[Indicar el requerimiento tecnológico o de procesos que se requiere para satisfacer la necesidad]*	Escenario *[Indicar la situación por la cual surge la necesidad]*	Impacto *[Indicar el análisis de impacto, incluyendo el mecanismo de evaluación y análisis]*

Necesidad *[Indicar la necesidad que tiene la Institución]*	Directriz de respuesta a incidentes *[Indicar el requerimiento tecnológico o de procesos que se requiere para satisfacer la necesidad]*	Escenario *[Indicar la situación por la cual surge la necesidad]*	Impacto *[Indicar el análisis de impacto, incluyendo el mecanismo de evaluación y análisis]*

Firmas y fecha de elaboración, revisión y aprobación de la directriz para la administración de riesgos a la seguridad de la información

Fecha de Elaboración: *(DD/MM/AAAA)*

Firma	*Firma*	*Firma*
Nombre	*Nombre*	*Nombre*
Cargo	*Cargo*	*Cargo*
Elaboró	**Revisó**	**Aprobó**

3. ANÁLISIS DE COSTO-BENEFICIO DE CONTROLES DE SEGURIDAD:

Objetivo y alcance de la evaluación

[Objetivo: Considerar exclusivamente la lista de escenarios cuya estrategia de seguridad implica el uso de controles o la modificación del proceso, esto es, solo aquellos escenarios de riesgo que deban ser evitados, prevenidos, mitigados o financiados.
Alcance: Se limita a aquellos factores principales, cuyo cálculo relativamente sencillo permite obtener una aproximación de los costos involucrados en un escenario de riesgo, donde predominan los factores probabilísticas.]

Tabla de Análisis de Costo - Beneficio

Código Escenario	Prioridad	R	Control	Costo (B)	P	I$	R$	¿Control aceptable? B<=R$	P'	I'	R'	¿Control conveniente? R>R'	¿Se recomienda?	Inversión
													Total: $	

R: riesgo
B: valor económico del control
P: Probabilidad de ocurrencia
I$: Impacto en recursos económicos
R$: valor económico del riesgo
P': probabilidad de ocurrencia después de implementar el control
I': Impacto después de implementar el control
R': Riesgo residual (después de implementar el control)

Instrucciones de llenado:

1. *Anotar en la primera fila el código de escenario de riesgo de máxima prioridad, junto con sus valores de "prioridad", "R", y "P", así como el "Control" propuesto de mayor valor.*
2. *Anotar, en las filas siguientes, los mismos datos para aquellos escenarios a los que les aplica el mismo Control de la primera fila.*
3. *Continuar con el escenario de mayor prioridad de entre los que aún no se han considerado.*
4. *Ejecutar los pasos 1, 2 y 3, hasta agotar todos los escenarios.*
5. *Para cada escenario, investigar el Costo del control (B), considerando para ello costos de adquisición o desarrollo, instalación, mantenimiento, capacitación, soporte técnico, etc.).*
6. *Investigar y consensuar el impacto "I$", desde un punto de vista exclusivamente financiero y con la mayor precisión posible (considerar costos de inventario, pérdidas por procesos interrumpidos, costos de recuperación de imagen, datos, hardware, software, etc.).*
7. *Calcular "R$" (riesgo en función de costos) mediante el producto de "P" por "I$".*
8. *Comparar costos entre "B" y "R$";*
    a. *Si "B" es menor o igual a "R$", el control es aceptable.*
    b. *Si "B" es mayor a "R$", rechazar el control y reiniciar el proceso al mismo escenario, con un control diferente, incluyendo aquellos escenarios a los que le aplique el nuevo control.*
9. *Recalcular "P" (ahora P'), pero tomando en cuenta la influencia del control ya aceptado.*
10. *Recalcular I' para estar en posibilidades de obtener el valor de R', al multiplicar P' por I'.*

11. *Verificar si R es ahora menor que R', en cuyo caso se considera que el control es conveniente y se recomienda. En caso contrario, deberá reiniciar el cálculo.*

12. *Registrar los costos de todos los controles recomendados y obtener el total a invertir.*

13. *Continuar con el llenado de la Tabla de Reproceso de análisis Costo - Beneficio, capturando los códigos de los escenarios en el orden de su prioridad original.*

14. *Asignar a cada escenario el valor de su riesgo residual (R').*

15. *De acuerdo a su nuevo riesgo residual, asignar nuevamente prioridades.*

16. *Proponer nuevos controles para aquellas prioridades elevadas, y, de ser el caso, reiniciar el análisis costo beneficio.*

Consideraciones:

Las actividades a realizar consisten en obtener y comparar dos valores: el valor económico del control propuesto, y el correspondiente a la pérdida ocasionada por la materialización de la amenaza, es decir, el nivel de impacto en términos financieros.

Un control cumple con la característica de “aceptabilidad”, si su costo es menor o igual al producto de la probabilidad de ocurrencia de la amenaza, por el costo económico generado en la dependencia o entidad como consecuencia de la materialización de la amenaza. En el caso de que un mismo control se repita en más de un escenario, su nivel de aceptabilidad se incrementará al comparar su costo, contra la sumatoria de los productos de la probabilidad de ocurrencia por el costo económico de los diversos riesgos enfrentados.

Para la obtención del valor económico del control propuesto, se deben considerar todos los costos posibles incluyendo: adquisición o desarrollo, instalación (material y mano de obra), mantenimiento (durante el primer año como referencia), capacitación, soporte técnico, etc. Para la obtención del nivel de impacto en términos financieros (valor económico de la pérdida ocasionada por la materialización de la amenaza), los costos a considerar deben involucrar: valor de inventario del activo, pérdidas por procesos interrumpidos, costo de recuperación de imagen, datos, hardware y software (instalación, tiempo, recursos humanos, etc.). Una vez realizadas las comparaciones entre “B" y “R”, se cuenta con los elementos de juicio necesarios para determinar cuáles son los controles, que en un primer esfuerzo se recomienda implementar. Los criterios que sirven de base para emitir estas recomendaciones están en función de:

Las prioridades de los escenarios de riesgo; y

La relación costo-beneficio.

Es necesario repetir la última parte del procedimiento, con el fin de actualizar el valor del riesgo al considerar ahora los controles que ya se han recomendado. Así, será necesario determinar nuevamente “P” e “I” (tomando en cuenta la existencia del nuevo control), y calcular “R” esperando que ahora su valor sea igual o menor a 1.8, de forma tal que se haya transformado en un riesgo del tipo aceptable. En el caso de que aún tenga un valor mayor, se establece su nueva prioridad y se determina la nueva estrategia a seguir, a fin de tomar alguna de las siguientes decisiones:

Proponer un control diferente en sustitución del previo (prioridad máxima o igual a la prioridad original);

Proponer un control adicional (prioridad media o menor a la prioridad original); y

Asumir el riesgo residual (prioridad mínima).

Tabla de Reproceso de análisis Costo – Beneficio

Código escenario	Prioridad original	Riesgo residual	Nueva prioridad	Nuevos controles presupuestos

Firmas y fecha de elaboración, revisión y aprobación del Análisis de costo-beneficio de controles de seguridad

Fecha de Elaboración: *(DD/MM/AAAA)*

Firma	*Firma*	*Firma*
Nombre	*Nombre*	*Nombre*
Cargo	*Cargo*	*Cargo*
Elaboró	**Revisó**	**Aprobó**

4. DECLARACIONES DE APLICABILIDAD:

Identificación de la Declaración de aplicabilidad (SoA) *[1…]*	*[Indicar el número de identificación y nombre corto de la Declaración de Aplicabilidad (SoA).]*
Identificación de la Declaración de aplicabilidad (SoA) *[2…]*	*[Indicar el número de identificación y nombre corto de la Declaración de Aplicabilidad (SoA).]*
Identificación de la Declaración de aplicabilidad (SoA) *[3…]*	*[Indicar el número de identificación y nombre corto de la Declaración de Aplicabilidad (SoA).]*
Identificación de la Declaración de aplicabilidad (SoA) *[4…]*	*[Indicar el número de identificación y nombre corto de la Declaración de Aplicabilidad (SoA).]*
Identificación de la Declaración de aplicabilidad (SoA) *[5…]*	*[Indicar el número de identificación y nombre corto de la Declaración de Aplicabilidad (SoA).]*

Riesgos:

[Deberá seguirse la Guía de identificación y evaluación de escenarios de riesgo, que se presenta en este mismo documento.]

Número de Riesgo *[1…]*	*[Indicar el número de riesgo asignado en la matriz de riesgos de TIC.]*
Descripción	*[Descripción del riesgo, indicando el activo y el riesgo asociado.]*
Evaluación	*[Indicar el nivel de riesgo obtenido.]*
Número de Riesgo *[2…]*	*[Indicar el número de riesgo asignado en la matriz de riesgos de TIC.]*
Descripción	*[Descripción del riesgo, indicando el activo y el riesgo asociado.]*
Evaluación	*[Indicar el nivel de riesgo obtenido.]*
Número de Riesgo *[3…]*	*[Indicar el número de riesgo asignado en la matriz de riesgos de TIC.]*
Descripción	*[Descripción del riesgo, indicando el activo y el riesgo asociado.]*
Evaluación	*[Indicar el nivel de riesgo obtenido.]*
Número de Riesgo *[4…]*	*[Indicar el número de riesgo asignado en la matriz de riesgos de TIC.]*
Descripción	*[Descripción del riesgo, indicando el activo y el riesgo asociado.]*
Evaluación	*[Indicar el nivel de riesgo obtenido.]*

Controles implantados					
Control *[Indicar la identificación y el nombre del control]*	Responsable *[Indicar el responsable del control]*	Descripción *[Señalar las características del control implementado]*	Tipo *[Indicar si es un control de detección o de prevención]*	Frecuencia *[Indicar la periodicidad con que se realizará el control]*	Justificación *[Indicar la justificación para el control implantado]*

Controles a implantar para la mitigación del riesgo					
Control seleccionado *[Indicar la identificación y el nombre del control]*	Responsable *[Indicar el responsable del control]*	Descripción *[Señalar la características del control a implementar]*	Tipo *[Indicar si es un control de detección o de prevención]*	Frecuencia *[Indicar la periodicidad con que se realizará el control]*	Justificación *[Indicar la justificación para la implementación del control]*

Documentación de soporte de las Declaraciones de aplicabilidad

[Integrar la relación de la documentación que sustenta las definiciones de las Declaraciones de aplicabilidad, y anexar a este producto, los estudios, análisis y documentos de trabajo que las sustenten.]

5. PROGRAMA DE MITIGACIÓN DE RIESGOS:

Identificación del Programa	*[Indicar el número de identificación y nombre corto del Programa de implantación de controles para reducir el impacto de un riesgo de acuerdo a la estrategia que se decida: evitar, mitigar, transferir o aceptar.]*

[Considerar para cada riesgo la elaboración de la tabla siguiente, constituyéndose la totalidad de tablas en el Programa de mitigación de riesgos.]

Número de Riesgo	*[Indicar el número de identificación del riesgo de acuerdo a la Matriz de riesgos de TIC.]*
Descripción	*[Proporcionar una descripción breve del riesgo, indicado el activo de TIC afectado.]*
Impacto	*[Proporcionar una descripción breve del impacto que causaría a la Institución el riesgo.]*
Controles Asociados	*[Indicar los controles a implementar y su relación con el riesgo en cuestión para llevar a cabo su mitigación.]*
Fecha de implementación	*[Proporcionar la fecha de implementación del o los controles.]*
Responsable de la implantación	*[Indicar responsable de la implantación del Programa.]*
Responsable de verificar el cumplimiento	*[Indicar responsable de realizar la actividad de verificación del cumplimiento del Programa.]*

Actividades a realizar					
Número Actividad *[Indicar el número de la actividad]*	Responsable *[Indicar responsable de realizar la actividad]*	Descripción *[Indicar las tareas que se realizarán en la actividad]*	Fecha inicio *[Indicar la fecha en que se iniciará la actividad]*	Fecha final *[Indicar la fecha en que se terminará la actividad]*	Justificación *[Indicar las bases de la decisión de realizar la actividad]*

Firmas y fechas de elaboración, revisión y autorización del programa de mitigación de riesgos

Fecha de Elaboración: *(DD/MM/AAAA)*

Firma	*Firma*	*Firma*
Nombre	*Nombre*	*Nombre*
Cargo	*Cargo*	*Cargo*
Elaboró	**Revisó**	**Aprobó**

6. PROGRAMA DE CONTINGENCIA DE RIESGOS:

Objetivo del Programa

[Documentar las acciones y decisiones en caso de un evento o incidente que tenga un impacto potencial para la Institución.]

Eventos generadores

[Indicar los eventos que pueden propiciar el despliegue del Programa de contingencia. Indicar las acciones o mecanismos de activación del Programa de contingencia.]

[Para cada riesgo se debe especificar:]

Definición del Programa de contingencia y pruebas de viabilidad

[Realizar un matriz de pruebas indicando las actividades y resultados obtenidos para la solución del incidente.]

Definición de la estructura del equipo de respuesta a la contingencia por el riesgo

[Indicar las áreas participantes, con los responsables del seguimiento y aseguramiento de la ejecución del Programa de contingencia por el riesgo materializado.]

Responsabilidades de cada integrante

[Indicar las responsabilidades de los integrantes del equipo de respuesta: nombre completo, cargo, ubicación, control involucrado, activo de información, entre otros.]

Aseguramiento de respuesta a la contingencia

[Establecer los mecanismos y medidas para que la respuesta inicial sea de forma segura, ejemplo los turnos de guardia, permisos y acceso a las instalaciones.]

Control de versiones del Programa de contingencia

[Indicar los cambios que se han realizado al Programa, indicando la fecha, la versión, sección modificada, descripción del cambio, nombre y firma de quien realizó, autorizó y valido la nueva versión.]

Evaluación preliminar del daño

[Describir las tareas a realizar para poder identificar y evaluar el nivel de contingencia que se presenta indicando el grado de daño de los activos afectados por el incidente.]

Informar a los usuarios afectados por la contingencia

[Después de realizar un análisis del resultado de las tareas que nos indican el nivel de contingencia que se tiene, transmitir por los medios de comunicación acordados, al personal y áreas afectadas la contingencia de que se trata y la estimación de solución.]

Procedimiento de respuesta

[Describir las medidas técnicas, organizativas y humanas a realizar para la solución del incidente de manera pronta y eficiente, es el Procedimiento de movilización de las partes involucradas.]

Ejecución

[Describir las tareas necesarias a realizar por cada una de las áreas involucradas para la solución de los incidentes.]

Evaluación

[Efectuar un análisis de los resultados de la aplicación del Programa de contingencia y elaborar un informe describiendo los daños generados por el incidente, el alcance de reparación obtenido y acciones de mejora sobre el programa ejecutado.]

Lista de contactos externos

[Indicar el nombre de empresa, dirección o área involucrada en el Programa de contingencia que sea externa, considerado el nombre de la empresa, personal de contacto y medios de contacto.]

Firmas y fechas de elaboración, revisión y autorización del programa de contingencia de riesgos

Fecha de Elaboración: *(DD/MM/AAAA)*

Firma	*Firma*	*Firma*
Nombre	*Nombre*	*Nombre*
Cargo	*Cargo*	*Cargo*
Elaboró	**Revisó**	**Aprobó**

7. PROGRAMA DE IMPLANTACIÓN PARA EL MANEJO DE RIESGOS:

[Para cada uno de los controles de seguridad para el manejo de los riesgos identificados, elaborar las siguientes tablas:]

Identificación del Programa	*[Indicar el número de identificación y nombre corto del Programa de implantación de controles para reducir un riesgo a niveles aceptables.]*

Número de Riesgo	*[Indicar el número de identificación del riesgo de acuerdo a la Matriz de riesgos.]*
Descripción	*[Proporcionar una descripción breve del riesgo, indicado el activo afectado.]*
Impacto	*[Proporcionar una descripción breve del impacto que causaría a la Institución el riesgo.]*
Controles Asociados	*[Indicar los controles a implantar y su relación con el riesgo en cuestión para llevar a cabo su mitigación.]*
Fecha de implementación	*[Proporcionar la fecha de implantación del o los controles.]*
Responsable de la implantación	*[Indicar responsable de la implantación del Programa.]*
Responsable de verificar el cumplimiento	*[Indicar responsable de realizar la actividad de verificación del cumplimiento del Programa.]*

Actividades a realizar					
Número Actividad *[Indicar el número de la actividad]*	Responsable *[Indicar responsable de realizar la actividad]*	Descripción *[Indicar las tareas que se realizarán en la actividad]*	Fecha inicio *[Indicar la fecha en que se iniciará la actividad]*	Fecha final *[Indicar la fecha en que se terminará la actividad]*	Justificación *[Indicar las bases de la decisión de realizar la actividad]*

Firmas y fechas de elaboración, revisión y autorización del programa implantación para el manejo de riesgos

Fecha de Elaboración: *(DD/MM/AAAA)*

Firma	*Firma*	*Firma*
Nombre	*Nombre*	*Nombre*
Cargo	*Cargo*	*Cargo*
Elaboró	**Revisó**	**Aprobó**

Firmas y fechas de elaboración, revisión y autorización del apartado Documento de resultados del Análisis de riesgos

Fecha de Elaboración: *(DD/MM/AAAA)*

Firma	*Firma*	*Firma*
Nombre	*Nombre*	*Nombre*
Cargo	*Cargo*	*Cargo*
Elaboró	**Revisó**	**Aprobó**

8. LISTA DE AMENAZAS A ACTIVOS DE INFORMACIÓN (CATÁLOGO DE AMENAZAS BASE)

Número referencia	Amenaza	Agente Amenaza
1001	Incendio	Material (falla)
1002	Incendio	Natural
1003	Incendio	Delincuencia organizada
1004	Incendio	Grupo subversivo
1005	Incendio	Personal interno descontento(intencional)
1006	Incendio	Personal interno inexperto (accidental)
1007	Incendio	Proveedor / Contratista
1008	Incendio	Comunidad
1009	Incendio	Grupo terrorista
1010	Incendio	Milicia extranjera
1011	Incendio	Servicios inteligencia / contrainteligencia
1012	Incendio	Ex-empleado
1013	Sismo	Natural
1014	Erupción volcánica	Natural
1015	Huracán / Tormenta	Natural
1016	Inundación	Material (falla)
1017	Inundación	Natural
1018	Rayos	Natural
1019	Interrupción energía eléctrica	Material (falla)
1020	Interrupción energía eléctrica	Natural
1021	Interrupción energía eléctrica	Delincuencia organizada
1022	Interrupción energía eléctrica	Grupo subversivo
1023	Interrupción energía eléctrica	Personal interno descontento (intencional)
1024	Interrupción energía eléctrica	Personal interno inexperto (accidental)
1025	Interrupción energía eléctrica	Proveedor / Contratista
1026	Interrupción energía eléctrica	Comunidad
1027	Interrupción energía eléctrica	Grupo terrorista

1028	Interrupción energía eléctrica	Milicia extranjera
1029	Interrupción energía eléctrica	Servicios inteligencia / contrainteligencia
1030	Interrupción energía eléctrica	Ex-empleado
1031	Chantaje	Delincuencia organizada
1032	Chantaje	Grupo subversivo
1033	Chantaje	Personal interno descontento (intencional)
1034	Chantaje	Proveedor / Contratista
1035	Chantaje	Comunidad
1036	Chantaje	Grupo terrorista
1037	Chantaje	Milicia extranjera
1038	Chantaje	Servicios inteligencia / contrainteligencia
1039	Chantaje	Ex-empleado
1040	Extorsión	Delincuencia organizada
1041	Extorsión	Grupo subversivo
1042	Extorsión	Personal interno descontento (intencional)
1043	Extorsión	Proveedor / Contratista
1044	Extorsión	Comunidad
1045	Extorsión	Grupo terrorista
1046	Extorsión	Milicia extranjera
1047	Extorsión	Servicios inteligencia / contrainteligencia
1048	Extorsión	Ex-empleado
1049	Atentado	Delincuencia organizada
1050	Atentado	Grupo subversivo
1051	Atentado	Personal interno descontento (intencional)
1052	Atentado	Proveedor / Contratista
1053	Atentado	Comunidad
1054	Atentado	Grupo terrorista
1055	Atentado	Milicia extranjera
1056	Atentado	Servicios inteligencia / contrainteligencia
1057	Atentado	Ex-empleado
1058	Robo	Delincuencia organizada
1059	Robo	Grupo subversivo
1060	Robo	Personal interno descontento (intencional)
1061	Robo	Proveedor / Contratista
1062	Robo	Comunidad
1063	Robo	Grupo terrorista
1064	Robo	Milicia extranjera
1065	Robo	Servicios inteligencia / contrainteligencia
1066	Robo	Ex-empleado
1067	Fraude	Delincuencia organizada
1068	Fraude	Grupo subversivo
1069	Fraude	Personal interno descontento (intencional)
1070	Fraude	Personal interno inexperto (accidental)
1071	Fraude	Proveedor / Contratista
1072	Fraude	Comunidad
1073	Fraude	Grupo terrorista
1074	Fraude	Milicia extranjera
1075	Fraude	Servicios inteligencia / contrainteligencia
1076	Fraude	Ex-empleado
1077	Motín	Personal interno descontento (intencional)
1078	Sabotaje	Delincuencia organizada
1079	Sabotaje	Grupo subversivo
1080	Sabotaje	Personal interno descontento (intencional)
1081	Sabotaje	Personal interno inexperto (accidental)
1082	Sabotaje	Proveedor / Contratista
1083	Sabotaje	Comunidad
1084	Sabotaje	Grupo terrorista
1085	Sabotaje	Milicia extranjera
1086	Sabotaje	Servicios inteligencia / contrainteligencia

1087	Sabotaje	Ex-empleado
1088	Incumplimiento	Proveedor / Contratista
1089	Insolvencia	Proveedor / Contratista
1090	Acceso no autorizado	Hacker
1091	Acceso no autorizado	Delincuencia organizada
1092	Acceso no autorizado	Grupo subversivo
1093	Acceso no autorizado	Personal interno descontento (intencional)
1094	Acceso no autorizado	Personal interno inexperto (accidental)
1095	Acceso no autorizado	Proveedor / Contratista
1096	Acceso no autorizado	Comunidad
1097	Acceso no autorizado	Grupo terrorista
1098	Acceso no autorizado	Milicia extranjera
1099	Acceso no autorizado	Servicios inteligencia / contrainteligencia
1100	Acceso no autorizado	Ex-empleado
1101	Acceso no autorizado	Script Kiddies
1102	Ingeniería social	Hacker
1103	Ingeniería social	Delincuencia organizada
1104	Ingeniería social	Grupo subversivo
1105	Ingeniería social	Personal interno descontento (intencional)
1106	Ingeniería social	Proveedor / Contratista
1107	Ingeniería social	Comunidad
1108	Ingeniería social	Grupo terrorista
1109	Ingeniería social	Milicia extranjera
1110	Ingeniería social	Servicios inteligencia / contrainteligencia
1111	Ingeniería social	Ex-empleado
1112	Ingeniería social	Script Kiddies
1113	Código malicioso	Hacker
1114	Código malicioso	Delincuencia organizada
1115	Código malicioso	Grupo subversivo
1116	Código malicioso	Personal interno descontento (intencional)
1117	Código malicioso	Personal interno inexperto (accidental)
1118	Código malicioso	Proveedor / Contratista
1119	Código malicioso	Comunidad
1120	Código malicioso	Grupo terrorista
1121	Código malicioso	Milicia extranjera
1122	Código malicioso	Servicios inteligencia / contrainteligencia
1123	Código malicioso	Ex-empleado
1124	Código malicioso	Script Kiddies
1125	Suplantación de identidad	Hacker
1126	Suplantación de identidad	Delincuencia organizada
1127	Suplantación de identidad	Grupo subversivo
1128	Suplantación de identidad	Personal interno descontento (intencional)
1129	Suplantación de identidad	Personal interno inexperto (accidental)
1130	Suplantación de identidad	Proveedor / Contratista
1131	Suplantación de identidad	Comunidad
1132	Suplantación de identidad	Grupo terrorista
1133	Suplantación de identidad	Milicia extranjera
1134	Suplantación de identidad	Servicios inteligencia / contrainteligencia
1135	Suplantación de identidad	Ex-empleado
1136	Suplantación de identidad	Script Kiddies
1137	Negación de servicio	Hacker
1138	Negación de servicio	Delincuencia organizada
1139	Negación de servicio	Grupo subversivo
1140	Negación de servicio	Personal interno descontento (intencional)
1141	Negación de servicio	Personal interno inexperto (accidental)
1142	Negación de servicio	Proveedor / Contratista
1143	Negación de servicio	Comunidad
1144	Negación de servicio	Grupo terrorista
1145	Negación de servicio	Milicia extranjera

1146	Negación de servicio	Servicios inteligencia / contrainteligencia
1147	Negación de servicio	Ex-empleado
1148	Negación de servicio	Script Kiddies
1149	Crackeo de contraseñas	Hacker
1150	Crackeo de contraseñas	Delincuencia organizada
1151	Crackeo de contraseñas	Grupo subversivo
1152	Crackeo de contraseñas	Personal interno descontento (intencional)
1153	Crackeo de contraseñas	Personal interno inexperto (accidental)
1154	Crackeo de contraseñas	Proveedor / Contratista
1155	Crackeo de contraseñas	Comunidad
1156	Crackeo de contraseñas	Grupo terrorista
1157	Crackeo de contraseñas	Milicia extranjera
1158	Crackeo de contraseñas	Servicios inteligencia / contrainteligencia
1159	Crackeo de contraseñas	Ex-empleado
1160	Crackeo de contraseñas	Script Kiddies
1161	Modificación de datos	Hacker
1162	Modificación de datos	Delincuencia organizada
1163	Modificación de datos	Grupo subversivo
1164	Modificación de datos	Personal interno descontento (intencional)
1165	Modificación de datos	Personal interno inexperto (accidental)
1166	Modificación de datos	Proveedor / Contratista
1167	Modificación de datos	Comunidad
1168	Modificación de datos	Grupo terrorista
1169	Modificación de datos	Milicia extranjera
1170	Modificación de datos	Servicios inteligencia / contrainteligencia
1171	Modificación de datos	Ex-empleado
1172	Modificación de datos	Script Kiddies

9. GUÍA DE IDENTIFICACIÓN Y EVALUACIÓN DE ESCENARIOS DE RIESGO

Objetivo:

Efectuar los cálculos necesarios que permitan establecer el valor relativo del riesgo para cada escenario planteado, de acuerdo a la secuencia que se define en la presente guía.

Alcance:

[Definir el ámbito de aplicación y alcance de la Identificación y evaluación de escenarios de riesgo.]

Para determinar el valor de “P” e “I”, se deben utilizar tres valores en cada una de las siguientes tablas:

Tabla 1. *Probabilidad de ocurrencia*

Valor	Probabilidad de ocurrencia de la amenaza	Homologación al Manual de Control Interno
0.9	Alta	6-10
0.5	Media	2-5
0.1	Baja	1

Tabla 2. ***Nivel de impacto***

Valor	Impacto
100	Alto
50	Medio
10	Bajo

Utilizando la fórmula y las tablas antes mostradas, se está en posibilidad de determinar el valor del riesgo de una forma sencilla, pueden aplicarse dos estrategias para obtener mayor precisión en los valores de riesgo que se calculen:

- Incluir factores adicionales que ejercen influencia en la probabilidad de ocurrencia, e
- Incrementar la cantidad de valores a considerar para las ponderaciones en las tablas.

Con base en lo anterior, la fórmula que se establece como: P=(e+i+c+v)/4

Donde:

"P".- Probabilidad de ocurrencia.
"e".- Existencia de un agente amenaza desde la perspectiva de un activo de información particular (existir).
"i".- Interés del agente amenaza para atacar al activo de información (querer).
"c".- Capacidad del agente amenaza para atacar al activo de información (poder).
"v".- Vulnerabilidad del activo de información.

Nota: Cada variable e, i, c y v influye **en igual proporción**.

Considerando la Nota anterior, este modelo permite realizar estimaciones básicas de los escenarios, utilizando inicialmente un criterio conservador. A medida que éste se utilice, puede ajustar el modelo, con base en los resultados que se obtengan de su aplicación y constante evaluación.

Para la ponderación de los valores requeridos en esta fórmula, se propone el uso de las tablas siguientes:

Tabla 3. ***Existencia del agente amenaza para el cálculo de P.***

Valor	Probabilidad de existencia del agente amenaza
0.9	Es casi seguro que existe
0.7	Es muy posible que exista
0.5	Es probable que exista
0.3	Es poco probable que exista
0.1	Es casi imposible que exista

Tabla 4. ***Niveles de Interés del agente amenaza para el cálculo de P.***

Valor	Nivel de interés del agente amenaza
0.9	El interés es incontrolable
0.7	Se genera mucho interés
0.5	Se genera regular interés
0.3	Se genera poco interés
0.1	Casi no se genera interés

Tabla 5. ***Capacidad del agente amenaza para el cálculo de P.***

Valor	Nivel de capacidad del agente amenaza
0.9	Los recursos son superiores
0.7	Cuenta con muchos recursos

0.5	Los recursos son regulares
0.3	Cuenta con muy pocos recursos
0.1	Los recursos son casi nulos

Tabla 6 ***Vulnerabilidad del Activo de información para el cálculo de P.***

Valor	Vulnerabilidad del activo de información
0.9	Sin ningún tipo de protección
0.7	Muy poca protección
0.5	Medianamente protegido
0.3	Protección normal
0.1	Protección reforzada

Una vez que se ha visto como obtener el valor de "P", debe obtenerse el valor del impacto (I), refiriéndose a la Tabla 7 (los valores de esta tabla pueden ser modificados de acuerdo a las necesidades de cada Institución).

Tabla 7. ***Nivel de impacto para el cálculo de R.***

	Impacto	Humano	Material	Financiero	Operativo	Imagen
10	Desastroso	Muertes	Pérdidas graves no recuperables	Más de $1,000,000.00	Afectación de procesos críticos que no pueden restablecerse en menos de dos días	Difusión a nivel internacional
8	Gran impacto	Heridos	Pérdidas graves recuperables a largo plazo	Entre $100,000.00 y $1,000,000.00	Afectación de procesos críticos, que pueden restablecerse en menos de dos días	Difusión a nivel nacional
6	Regular impacto	Lesiones que producen una incapacidad	Pérdidas leves no recuperables	Entre $50,000.00 y $100,000.00	Afectación de varios procesos no críticos	Difusión a nivel local
4	Mínimo impacto	Lesiones leves	Pérdidas leves recuperables	Entre $10,000.00 y $50,000.00	Afectación de un proceso no crítico	Difusión dentro de la dependencia o entidad
2	Insignificante	Sin lesiones	Sin pérdidas materiales	Menor de $10,000.00	Sin afectación de procesos	Difusión dentro de la unidad

Una vez evaluado cada uno de los cincos tipos de impacto, únicamente se utilizará el valor más alto que se haya obtenido, a fin de sustituirlo en la fórmula principal R= PI.

De esta manera, se tiene la certeza de que se han considerado los posibles impactos desde diferentes perspectivas y no únicamente con base en las primeras impresiones (fenómeno que tiende a presentarse cuando se realizan tareas mentales repetitivas, como lo es en este caso, la ponderación del impacto para una gran cantidad de amenazas).

Es importante resaltar que el cálculo de P con base en los cuatro factores (e, i, c y v), solo se aplica para aquellos casos en que participe el elemento humano como agente perpetrador. En otros casos no se considera el interés (i). Así, al tratarse de amenazas naturales (medio ambiente), o materiales (incendio), la fórmula a emplearse se reduce a la siguiente: P= (e+c+v)/3

El análisis y determinación de riesgos, se resume como la realización de dos actividades primordiales: el establecimiento de los escenarios de riesgo (cada uno de los activos de información se relaciona con cada amenaza y su respectivo agente), mediante la "Tabla de Análisis y Determinación de Riesgos" mostrada a continuación; y el consenso de valores asignados a

cada factor, se sugiere el empleo del método "Delphi". Todo ello para poder finalmente calcular el valor relativo del riesgo.

Consensuar valores

[El Líder con apoyo del Grupo de trabajo deberá consensuar los valores a asignar a los diferentes factores requeridos (e, i, c, v) para el cálculo del riesgo (se sugiere aplicar algún método formal, como el método Delphi), para recabar los valores que se indican en la Tabla de Análisis y Determinación de Riesgos. En este apartado anote conclusiones, comentarios u observaciones relevantes adicionales a la elaboración de la tabla siguiente.]

Tabla de Análisis y Determinación de Riesgos:
(parte 1)

Código *[Codificar cada escenario de riesgo (R-1, R-2, Etc.)]*	**Amenaza** *[Anotar el número de referencia de la primera amenaza]*	**Activo** *[Anotar el número de referencia del primer activo afectado por la amenaza]*	**e** *[Anotar el valor resultante de la ponderación de la Tabla 3]*	**i** *[Anotar el valor resultante de la ponderación de la Tabla 4]*	**c** *[Anotar el valor resultante de la ponderación de la Tabla 5]*	**v** *[Anotar el valor resultante de la ponderación de la Tabla 6]*	**P** *[Anotar el valor resultante de la media aritmética de los valores "e", "i", "c" y "v"]*
R-1							
R-2							
R-3							
R-4							
R-5							
R-6							
:							
R-n							

(parte 2)

Código *[Codificar cada escenario de riesgo (R-1, R-2, Etc.)]*	**ih** *[Anotar el valor resultante de la ponderación de la tercera columna de la Tabla 7]*	**im** *[Anotar el valor resultante de la ponderación de la cuarta columna de la Tabla 7]*	**if** *[Anotar el valor resultante de la ponderación de la quinta columna de la Tabla 7]*	**io** *[Anotar el valor resultante de la ponderación de la sexta columna de la Tabla 7]*	**ii** *[Anotar el valor resultante de la ponderación de la séptima columna de la Tabla 7]*	**I** *[Anotar el valor más alto que se haya obtenido de las columnas "ih", "im", "if", "io" e "ii"]*	**R** *[Anotar el valor resultante del producto de "P" por "I"]*
R-1							
R-2							
R-3							
R-4							

R-5							
R-6							
:							
R-n							

e: existencia de agente amenaza
i: interés del agente amenaza
c: capacidad del agente amenaza
v: vulnerabilidades del activo de información
P: probabilidad de ocurrencia

ih: impacto humano
im: impacto material
if: impacto financiero
io: impacto operativo
ii: impacto de imagen
I: impacto

R: riesgo

Deberá:
1. En la columna P anotar el resultado de (e+i+c+v)/4.
2. En la columna I anotar el valor MAS ALTO de entre las columnas ih, im, if, io, ii.
3. En la columna R anotar el valor de PI.

Una vez que se cuenta con los valores de cada uno de los riesgos correspondientes a los diversos escenarios planteados, se debe proporcionar la siguiente información, que será requerida para soportar la posterior toma de decisiones:

- La relación de riesgos que no requieren ser atendidos.
- La relación de riesgos que si tienen que ser atendidos.
- El orden de prioridad para los riesgos que serán atendidos.
- La estrategia de seguridad a seguir.
- La relación de controles propuestos.

El criterio de aceptación para diferenciar los riesgos que requieren ser atendidos, de aquellos que pueden ser aceptados, se basa en el valor máximo que puede tener un riesgo cuyo impacto se ha ponderado como insignificante; esto es, la dependencia está dispuesta a asumir todos aquellos riesgos cuyo impacto ha sido evaluado con el mínimo valor, durante el análisis y determinación de riesgos.

Al representar mediante una matriz los diversos valores de riesgo posibles (Tabla 8), es posible observar que el máximo valor de un riesgo que ha sido ponderado como insignificante, es **1.8**. Este valor delimita entonces el rango de riesgos aceptables, por lo que todos aquellos riesgos cuyo valor sea igual o menor a **1.8**, no requieren de llevar a cabo acción alguna por parte de la dependencia o entidad.

Tabla 8. ***Matriz de riesgos.***

Probabilidad de Ocurrencia						
0.9	**Casi Seguro**	1.8	3.6	6.4	7.2	9
0.7	**Alta**	1.4	2.8	4.2	5.6	7
0.5	**Mediana**	1	2	3	4	5
0.3	**Baja**	0.6	1.2	1.8	2.4	3
0.1	**Casi imposible**	0.2	0.4	0.6	0.8	1
		Insignificante	**Significativo**	**Grave**	**Crítico**	**Desastroso**
		2	4	6	8	10
		IMPACTO				

Por otra parte, aquellos riesgos cuyo valor sea mayor a **1.8, si** tienen que ser atendidos, siendo necesario entonces establecer un nivel de prioridad para su atención.

El nivel de prioridad de cada riesgo está basado en su valor relativo, esto es, al escenario de riesgo cuyo valor relativo es el más alto, le corresponde la prioridad de 1, al riesgo con el segundo valor más alto, le corresponde la prioridad 2 y así

sucesivamente hasta completar todos los escenarios.

Una vez establecidas las prioridades, el siguiente paso es determinar la estrategia de seguridad a seguir para enfrentar el riesgo. Para ello, se consideran 5 distintas alternativas: evitar, prevenir, mitigar, financiar o asumir. Estas estrategias de seguridad deben evaluarse en el orden en que se han mencionado, ya que como se entenderá durante la descripción de cada una de ellas, los beneficios que representan son mayores para la primera alternativa, disminuyendo hasta ser casi nulos en la última de las estrategias.

Estrategias:

- **Evitar:** Se trata de implementar lo necesario para que la amenaza no se materialice. Esto sólo será posible si de los componentes del escenario de riesgo (causa - evento - consecuencia), es eliminado el único factor no probabilístico sobre el que se tiene control, esto es, el activo de información. De manera que, en este caso, la única manera de evitar que un riesgo ocurra es eliminando la actividad o proceso que, en un particular escenario de riesgo, represente el objeto o blanco de la amenaza. Por ejemplo, consideremos el siguiente escenario:

  Amenaza: Modificación
  Agente amenaza: Un hacker en la red
  Activo de información: Sitio Web de la dependencia o entidad.

  En este caso, el riesgo de que una página Web de la organización sea modificada por un hacker, se puede evitar eliminando al agente amenaza, pero esa es una situación fuera de nuestro alcance, por lo que la única forma factible de evitar este riesgo, sería no exponer el activo de información, es decir, no contar con un sitio Web.

  Definitivamente, la estrategia de "evitar', representa el extremo en el compromiso entre seguridad y funcionalidad, sin embargo, debe ser considerada al principio de la evaluación con el fin de asegurar que en primera instancia se intentó desaparecer por completo al riesgo. La pregunta a contestar para decidir el empleo de esta alternativa sería: ¿La dependencia o entidad se ve más afectada si se enfrenta a este riesgo, que si se enfrenta a las consecuencias de desactivar este activo de información?

- **Prevenir:** Estrategia que se enfoca en reducir el valor de "**P**" en la ecuación del riesgo. Esto se logra mediante la implementación de controles que ayuden a disminuir la probabilidad de ocurrencia (acciones preventivas), enfocándose para ello en afectar de manera negativa, y sea el interés o capacidad del agente amenaza, o vulnerabilidades de nuestro activo de información. Una forma de facilitar la toma de decisiones respecto a la conveniencia de esta estrategia, es con ayuda de la matriz mostrada en la tabla 8, mediante la cual se puede apreciar en qué magnitud se debe reducir "**P**", para ubicar al riesgo en una zona de aceptabilidad.

- **Mitigar:** Se trata de una estrategia enfocada en acciones correctivas, ya que los controles a implementarse intentarán reducir el valor de "**I**" en la ecuación del riesgo. Esta alternativa asume que la amenaza se ha materializado y que los esfuerzos deben encaminarse a una rápida respuesta, para que el impacto sea reducido al mínimo valor posible. Al igual que en la estrategia anterior, la matriz de la tabla 8 permite determinar la magnitud en que "**I**" debe reducirse para que el riesgo sea aceptable. La elección de la estrategia depende entonces, del resultado de la comparación entre las magnitudes en que se requeriría modificar a "**P**" e "**I**", para que el valor del riesgo sea igual o menor a **1.8**.

- **Financiar:** Estrategia que considera que ante una amenaza ya materializada, la dependencia o entidad ha resultado afectada con el nivel de impacto pronosticado, por lo que prevé controles que le permitan contar con los recursos financieros necesarios, para lograr una rápida recuperación ante las consecuencias negativas.

- **Asumir:** Ultima de las alternativas como estrategia de seguridad, en la cual no se emplea ningún tipo de control cuando se prefiere conservar el riesgo con su valor actual. Esto puede ser ocasionado por las limitantes que sufre la dependencia o entidad ante restricciones económicas, materiales o de personal, siempre y cuando ninguna de las alternativas anteriores satisfaga los mínimos requerimientos de seguridad, o como resultado del análisis costo-beneficio en el que se refleje que es más costoso implementar el control, que soportar el impacto por la materialización de la amenaza.

Finalmente, se sugiere aplicar nuevamente la técnica de “Tormenta de ideas” o el método “Delphi”, para que, en consenso, el grupo de trabajo proponga los controles a ser implementados en cada uno de los escenarios de riesgo, considerando lo siguiente:

- Que el tipo de control (preventivo, correctivo o de recuperación) debe corresponder al tipo de estrategia seleccionada;
- Que es posible (más no obligatorio), listar hasta tres controles por cada escenario, en orden de importancia; y
- Que un mismo control puede brindar la seguridad requerida en más de un escenario de riesgo.

Integrar la “Tabla de Evaluación de Riesgos”, con la información resultante, recopilada siguiendo los factores críticos que establece el proceso y actividad en curso.

Estrategia

[El Líder, con apoyo del Grupo de trabajo y, considerando la información de la Tabla 8 “Matriz de Riesgos”, deberá determinar el tipo de Estrategia aplicable:

- *Evitar: Determinar mediante consenso si es posible eliminar el activo de información sin afectar los procesos a los que apoya, con el beneficio de eliminar un riesgo sin necesidad de invertir en controles. Si la respuesta es negativa, evaluar la posición del riesgo respecto a la Matriz de Riesgos.*
- *Prevenir: Seleccionar esta estrategia si el riesgo está más cerca de la zona sombreada en el eje vertical.*
- *Mitigar: Seleccionar esta estrategia si la mayor cercanía es en el eje horizontal.*

En el caso de igual cercanía, se recomienda optar por la estrategia de "prevenir" (control para que no ocurra).]

Tabla de Evaluación de Riesgos

Código Escenario	**P** *[Anotar los valores de "P", de acuerdo al código de cada escenario (un escenario por fila)]*	**I** *[Anotar los valores de "I", de acuerdo al código de cada escenario (un escenario por fila)]*	**R** *[Anotar los valores de "R", de acuerdo al código de cada escenario (un escenario por fila)]*	**Criterio Aceptación** *[Comparar el valor de "R" con el criterio de aceptación propuesto por esta metodología (1.8)]*	**¿Requiere control?** *[Anotar que **SI** se requiere control, cuando el valor de "R" es mayor a 1.8. en caso contrario anotar **NO**]*	**Prioridad** *[Asignar prioridades, únicamente a todos los escenarios que **SI** requieren control, tomando como referencia el valor de "R" de mayor a menor]*	**Estrategia** *[Determinar su tipo en términos de “Evitar”, “Prevenir” o “Mitigar”]*	**Controles Propuestos** *[Mediante técnica de “Tormenta de ideas”, proponer controles y consensuar los mismos en el Grupo para la asignación de valores de efectividad: alto, medio o bajo]*
R-1				1.8				
R-2				1.8				
R-3				1.8				
. . .				1.8				
R-6				1.8				

P: probabilidad de ocurrencia I: impacto R: riesgo