PLAN DE IMPLEMENTACIÓN DE UN SGSI BASADO EN LA NORMA ISO 27001:2013 EN EL ÁMBITO DE LA ADMINISTRACIÓN PUBLICA ARGENTINA

Autor: Mgter. Ing. Bruno A. Roberti Ferri

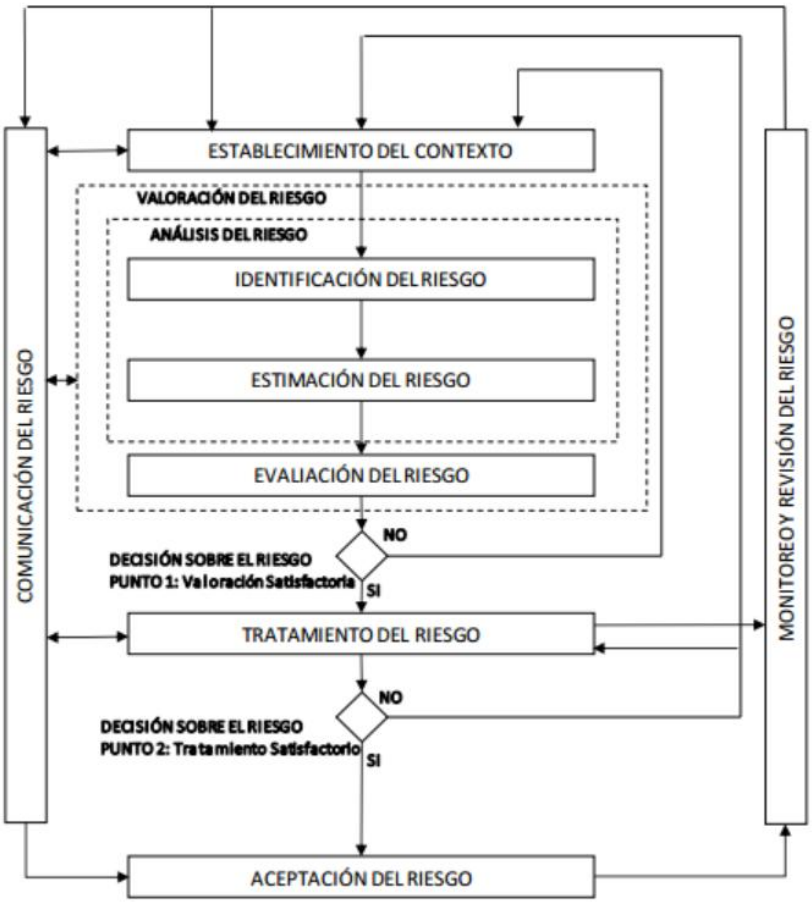
2.6 Metodología de Gestión del Riesgo

La realización de un análisis de Riesgos y su posterior tratamiento es un elemento imprescindible para la implementación de un Sistema de Gestión de la Seguridad de la Información. Teniendo en cuenta que la Disp. 1/2015 ONTI no indica una metodología en particular para el análisis de riesgo se ha optado por diseñar una que sea compatible con ISO 27005 y a la vez se adapte a las características del organismo.

La metodología propuesta se basa en activos, donde la identificación de los riesgos a los que estos están expuestos se realizará mediante la determinación de las amenazas existentes sobre los activos, para luego calcular la probabilidad y el impacto que van a causar.

Se ha tomado en cuenta la dificultad en la valoración de activos debido a la naturaleza de la organización y el enfoque en procesos de la Administración Pública Argentina para elegir una valoración cualitativa dentro de la metodología que proponemos.

Teniendo en cuenta los factores mencionados con anterioridad se propone que el cálculo del riesgo se realice teniendo en cuenta un análisis de las salvaguardas o controles implementados actualmente en el organismo, lo cual implica que el resultado del análisis arrojará un riesgo del tipo residual.



"Figura 8: Gestión de Riesgo de Seguridad ISO/IEC 27005"

La metodología cuenta con las siguientes etapas, adecuadas al estándar ISO 27005:

a. Identificación del Riesgo
    i. Identificación de activos
    ii. Clasificación de activos
    iii. Identificación de amenazas
    iv. Análisis de controles existentes
b. Estimación del Riesgo
    i. Análisis del impacto
    ii. Determinación del riesgo
c. Evaluación del Riesgo
d. Tratamiento de Riesgos

2.6.1 Identificación del Riesgo

El objetivo de este paso es conocer el nivel de exposición de los activos de información frente a las amenazas aplicables al entorno de funcionamiento de los procesos, es decir conocer los riesgos a los cuales se encuentra expuesto. Este paso incluye las siguientes etapas:

Identificación de activos: El primer paso para el análisis de riesgo es realizar el inventario de activos de información. Se entenderá por **activo de información/primarios** a cada sistema de información o aplicación informática utilizada para generar o manipular información del organismo. La otra categoría es la de los **activos de soporte**, los cuales refieren a activos físicos, activos de software, contenedores de datos, servicios de redes y telecomunicaciones e infraestructura tecnológica.

La dependencia entre activos se entiende en la medida que uno brinde servicios o soporte de algún tipo a otro, formando un árbol de dependencias que no implica jerarquía. Los activos incluidos en las categorías información son los que establecen los requisitos de seguridad para los otros los activos de soporte.

A cada activo se le asignará un propietario que deberá cumplir con las responsabilidades emanadas de la política de seguridad del organismo.

Clasificación de activos: La clasificación de los activos se realizará en base a la asignación de valores a tres dimensiones de la información: Confidencialidad (C), Integridad (I) y Disponibilidad (D). No se utilizaran criterios de valoración económica en el activo, pero si se identificará el tipo de proceso al que están asociados, siendo los valores de esta clasificación Sustantivo, Conducción y Apoyo en ese orden de importancia. El resultado de estas dimensiones nos dará una valoración del activo en función de la criticidad.

Los activos de soporte no serán clasificados, heredarán la criticidad del activo asociado al mismo, para el caso que sea más de uno se tomará la criticidad más alta entre todos los activos asociados. Cuando se trate de activos de redes o infraestructura se asignará la criticidad en base a la importancia en términos operativos de la unidad organizativa a la que presta servicio.

Identificación de amenazas: En el marco de esta metodología emplearemos la siguiente definición de amenaza: "Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

Para implementar esta metodología nos basaremos en el catálogo de amenazas propuesto por MAGERIT (Libro 2 "Catálogo de Elementos" - Punto 5), pero fusionando las categorías "Desastres Naturales" y "De origen industrial" en una sola llamada "Del Entorno". Por lo tanto las amenazas quedan clasificadas en los siguientes bloques:

- Del Entorno
- Errores y fallos no intencionados
- Ataques intencionados

Luego de identificar las amenazas que pueden afectar nuestros activos, se realizará una valoración las características de cada uno para determinar la Frecuencia. Entendiendo por frecuencia cuan probable o improbable es la materialización de la amenaza.

Análisis de Controles: Este paso busca reflejar de manera práctica la minimización de la probabilidad de la amenaza teniendo en cuenta la madurez de las salvaguardas. Se evalúa el grado de implementación de los controles, donde se tiene en cuenta si están implementados controles técnicos, controles organizativos y el grado de supervisión sobre ambos.

2.6.2 Estimación del Riesgo

El riesgo es una función del impacto y la probabilidad de ocurrencia de una amenaza. Este paso incluye las siguientes etapas:

Análisis del Impacto: Ese calculara el impacto teniendo en cuenta el valor del activo, proveniente del campo valoración de la clasificación del activo y la degradación estimada.

Determinación del Riesgo: Teniendo calculado el impacto y la probabilidad podemos calcular el riesgo de acuerdo a la fórmula

Riesgo = Impacto x Probabilidad

RIESGO		Frecuencia				
		MB	B	M	MA	A
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	B	B	B

"Figura 9: Matriz de calificación en función de Impacto y Probabilidad"

Aún se están ajustando los parámetros de esta estimación.

2.6.3 Evaluación del Riesgo

Como se ha indicado en el comienzo de este punto el análisis del riesgo va a contemplar los controles implementados por lo tanto ya es un análisis de Riesgo Residual y no es necesario calcular nuevamente el riesgo residual, hasta el próximo periodo indicado en la política de seguridad.

Propiedad del Riesgo: Dada la estructura del organismo, se designa como propietario de todos los riesgos al "Comité de Tecnología y Seguridad de la Información y Comunicaciones" (CoTySIC).

Nivel de Riesgo Aceptable: En este punto debemos determinar lo que se considera el nivel de riesgo aceptable para el organismo. El punto a partir del cual se debe proceder a realizar el tratamiento del riesgo.

Teniendo en cuenta un correcto equilibrio entre costo de protección y costo de exposición, la utilización del riesgo residual como criterio de estimación se fija un umbral de riesgo igual a Medio.

2.6.4 Tratamiento del Riesgo

Los riesgos que se encuentran por arriba del nivel aceptable de riesgo deben ser tratados eligiendo entre una de las siguientes 4 opciones:

Mitigarlo: Esta acción implica implantar los controles necesarios con el fin de que el nivel de riesgo disminuya a un punto que se encuentre bajo el límite aceptable. Para conseguir este objetivo se pueden realizar acciones preventivas o reducir el impacto de la amenaza. Esta es la primera opción por defecto que debe aplicar el organismo, las demás serán tratadas como excepciones.

Transferirlo: Mediante esta acción la organización comparte o traspasa a terceros el riesgo con el fin que sean éstos quienes puedan reducir su impacto o gestionar el riesgo de mejor

manera. Esta situación se presenta si el organismo no tiene los recursos o capacidad para mitigar el riesgo y no puede aceptarlo por la gravedad que representa. En el caso del organismo también puede darse esta opción cuando es indicado desde el poder ejecutivo nacional.

Evitarlo: Esta decisión implica tomar acciones tendientes a impedir que el riesgo se vuelva una realidad. Este puede realizarse mediante la sustitución del activo por uno que este dentro de un nivel de riesgo aceptable, o en última instancia no continuar la actividad relacionada con el activo.

Aceptarlo: Se entiende por aceptar un riesgo no realizar ninguna acción (de las 3 propuestas anteriormente) que permita evitar que se produzca. Esta decisión solo se debería tomar si no es posible ejecutar ninguna de las acciones anteriores, pero la probabilidad del mismo es baja o media-baja. La decisión de que la organización trabaje aceptando que está expuesta al riesgo si las probabilidades son mayores debe tomarse en forma excepcional y dejarse asentado en acta del comité.

Se realizará un documento de tratamiento de riesgos indicando la opción elegida y de medidas de seguridad de corresponder para todos los riesgos por encima del umbral.

La descripción detallada y aplicación de la presente metodología se incluye en el capítulo 3. Riesgos del presente trabajo.

3. ANÁLISIS DE RIESGOS

La realización de un análisis de Riesgos y su posterior tratamiento es un elemento imprescindible para la implementación de un Sistema de Gestión de la Seguridad de la Información. Se ha generado una metodología que sea compatible con ISO 27005 y a la vez se adapte a las características del organismo.

La metodología propuesta se basa en activos, donde la identificación de los riesgos a los que estos están expuestos se realizará mediante la determinación de las amenazas existentes sobre los activos, para luego calcular la probabilidad y el impacto que van a causar.

Se ha tomado en cuenta la dificultad en la valoración de activos debido a la naturaleza de la organización y el enfoque en procesos de la Administración Pública Argentina para elegir una valoración cualitativa dentro de la metodología que proponemos.

Teniendo en cuenta los factores mencionados con anterioridad se propone que el cálculo del riesgo se realice teniendo en cuenta un análisis de las salvaguardas o controles implementados actualmente en el organismo, lo cual implica que el resultado del análisis arrojará un riesgo del tipo residual.

3.1 Inventario de Activos

El primer paso para la gestión de riesgos es la identificación de los activos de información del organismo, los cuales se registraran dentro del inventario de acuerdo con las siguientes categorías:

- **Activo de información o primarios:** Aquí se incluirán todos los sistemas de información donde procesa información del organismo. No importa si los mismos son administrados dentro del organismo, o son parte de los que brinda el estado nacional para manejar aspectos centralizados de la gestión. En esta categoría no se realizará agrupamiento, pero no se trataran igual a todos sus elementos. Los activos del tipo "Externo" no se tomarán dentro del análisis de riesgo por no poder aplicar ningún control sobre los mismos y estar obligados a utilizarlos. En términos de gestión del riesgo los riesgos sobre esos activos son "Aceptados". Se incluyen en el inventario para identificar los contenedores de información del organismo y para formalizar quién es el funcionario encargada de autorizar el acceso a los mismos.
- **Activos de soporte:** Se ubican es esta categoría el Hardware, las aplicaciones, contenedores de datos (bases de datos, archivos, etc.), redes, Instalaciones, personal y servicios asociados a TIC's. Los activos de esta categoría se identificarán en grupos de elementos que comparten características similares para este estudio. Se tomará en cuenta naturaleza del activo, amenazas sobre el mismo y vulnerabilidades posibles para ese agrupamiento.

A su vez a los activos de información se les asignarán un subtipo, basado en la clasificación de procesos expuesta por la Sindicatura General de la Nación, de acuerdo al siguiente detalle:

Subtipos Activos de Información	
Sustantivos	Activos asociados a procesos que permiten el cumplimiento de los objetivos fundamentales de la organización, dando por resultado un producto (bien o servicio) que es recibido por el ciudadano/usuario, o por entes externos.
Conducción	Activos asociados a procesos destinados a dar sostén operativo para el cumplimiento de los objetivos de los procesos sustantivos.
Apoyo	Activos asociados a procesos dirigidos a organizar y facilitar la coordinación de la totalidad de los procesos de la organización (ejemplos: plan estratégico, gestión de riesgos, otros).
Externo	Sistemas asociados a todo tipo de proceso cuya administración no es llevada a cabo por el organismo, sin embargo brinda servicios y almacena datos relativos al organismo.

"Figura 11: Subtipos Activos de Información"

Para cada activo de información se le definirán los siguientes datos:

- Categoría: Tipo del activo de acuerdo con la figura 11.
- Identificación: Código alfanumérico de identificación única (Categ+Num).
- Nombre Activo: Identificación formal del activo para el organismo, generalmente se corresponde con el nombre del sistema pero hay excepciones.
- Proceso: Nombre del procesos de nivel superior al que presta servicio el activo
- Propietario: Unidad organizativa encargada de establecer los valores de disponibilidad, confidencialidad e integridad del activo. La responsabilidad siempre está en la máxima autoridad de la unidad mencionada.
- Responsable Operativo y Responsable Informático: Están asignados pero no se han colocado por un tema de confidencialidad
- Prioridad: Este valor se utiliza para calcular la criticidad del activo incluyendo otro factor además de los valores de DCI

Para los activos de soporte los subtipos son los siguientes:

Subtipos Activos de Soporte		
Hardware	HW	Equipos electrónicos que soportan directa o indirectamente los servicios que presta la organización.
Software	SW	Conjunto de componentes lógicos que contribuyen al procesamiento de la información. Por ejemplo: aplicaciones

		informáticas, software de sistemas. Están excluidos de esta categoría los activos de información
Infraestructura	IF	Instalaciones físicas y equipamiento que brinda soporte auxiliar al funcionamiento de los activos de hardware
Redes - Comunicaciones	RC	Servicios de comunicaciones propios y contratados para transportar información.
Contenedores Datos	CD	Dispositivos físicos o lógicos que permiten almacenar información.
Personal	P	Grupos de Personas relacionados con los sistemas de información.
Servicios	S	Todos los servicios contratados a un proveedor externo, exceptuando los asociados al tipo RC.

"Figura 12: Subtipos Activos de Soporte"

Para cada activo de soporte se le definirán los siguientes datos:

- Categoría: De acuerdo a lo descripto en la figura 12.
- Identificación: Código alfanumérico de identificación única (Categ+Num).
- Nombre Activo: Identificación del activo para el organismo.
- Activo de Información Relacionado
- Propietario
- Valoración
- Criticidad

La dependencia entre activos se generará en la medida que uno brinde servicios o soporte de algún tipo a otro, formando un árbol de dependencia que no implica jerarquía. Los activos de información dependerán de los activos de soporte, mientras que estos últimos pueden depender a su vez de otros activos de soporte.

3.2 Valoración de los Activos

No se utilizaran criterios de valoración económica en el activo de información, pero si se identificará el tipo de proceso al que están asociados, basada en la clasificación de procesos expuesta por la Sindicatura General de la Nación. Siendo los valores de esta clasificación Sustantivo, Conducción y Apoyo en ese orden de importancia. El resultado de esta priorización nos dará uno de los criterios de valoración del activo junto con la criticidad.

La escala de valores que se utilizará para la Confidencialidad es la siguiente:

Valor	Tipo
3	SUSTANTIVO
2	CONDUCCION
1	APOYO
0	EXTERNO

"Figura 13: Valoración Activos de Información"

La valoración de Activos de Información se compone de la siguiente fórmula

Valoración = Prioridad + Valor Criticidad

Mientras que para los Activos de Soporte se tomará el mismo criterio que con la Criticidad, heredando la mayor valoración de los activos de nivel superior a los que prestan soporte.

3.3 Clasificación de Activos

La clasificación de los activos se realizará en base a la asignación de valores a tres dimensiones de la información: Confidencialidad (C), Integridad (I) y Disponibilidad (D). Las dimensiones parten de los siguientes conceptos:

Dimensión	
Confidencialidad	Esta característica garantiza que la información contenida por el activo sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Integridad	Esta característica consiste en que la información del activo no ha sido modificada de manera no autorizada. Es la que salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Disponibilidad	Característica que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

"Figura 14: Dimensiones Seguridad de la Información"

Los activos de información serán clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen por el Propietario del activo

La escala de valores que se utilizará para la Confidencialidad es la siguiente:

Valor Confidencialidad	Nivel	Descripción
0	USO PÚBLICO	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleada del organismo o no.
1	USO RESERVADO-INTERNO	Información que puede ser conocida y utilizada por todos los empleados del organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el organismo, el Sector Público Nacional o terceros.
2	USO RESERVADO-CONFIDENCIAL	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al organismo, al Sector Público Nacional o a terceros.
3	USO RESERVADO-SECRETA	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros.

"Figura 15: Tabla valores Confidencialidad"

La escala de valores que se utilizará para la Integridad se define de la siguiente manera:

Valor Integridad	Nivel	Descripción
0	NO APLICA	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del organismo.
1	BAJO	Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el organismo, el Sector Público Nacional o terceros.
2	MEDIO	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el organismo, el Sector Público Nacional o terceros.
3	ALTO	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al organismo, al Sector Público Nacional o a terceros.

"Figura 16: Tabla valores Integridad"

La escala de valores que se utilizará para la Integridad se define de la siguiente manera:

Valor Disponibilidad	Nivel	Descripción
0	NO APLICA	Información cuya inaccesibilidad no afecta la operatoria del organismo.
1	BAJO	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el organismo, el Sector Público Nacional o terceros.
2	MEDIO	Información cuya inaccesibilidad permanente durante dos días podría ocasionar pérdidas significativas al organismo, al Sector Público Nacional o a terceros.
3	ALTO	Información cuya inaccesibilidad permanente durante seis horas podría ocasionar pérdidas significativas al organismo, al Sector Público Nacional o a terceros.

"Figura 17: Tabla valores Disponibilidad"

Calculo de la criticidad:

Valor Criticidad	Nivel	Descripción
De 0 a 3	BAJA	El activo interviene en procesos que no están directamente relacionados con el negocio, aunque son necesarios. Su indisponibilidad causa algún contratiempo pero en ningún caso se vería afectada la continuidad del negocio.
De 4 a 6	MEDIA	El activo interviene en procesos de apoyo a la organización. Su indisponibilidad puede retrasar un determinado proceso pero no se vería afectada la continuidad de negocio
De 7 a 9	ALTA	El activo interviene en procesos clave para la organización (aquellos que son necesarios y suficientes) y su no disponibilidad puede poner en peligro la continuidad del negocio o contiene información con implicaciones legales

"Figura 18: Tabla valores Criticidad"

Los activos de soporte heredarán la criticidad del activo asociado al mismo, para el caso que sea más de uno se tomará la criticidad más alta entre todos los activos asociados.

3.4 Tabla Resumen de Valoración

Del proceso realizado se obtiene un inventario valorizado y clasificado, similar al mostrado en la figura 19 para la categoría “Activos de Información”.

ID	NOMBRE	PROCESO	PROPIETARIO	PRIOR.	C	I	D	VALOR CRIT.	VALORACION	CRITICIDAD
IS1	XXX	1	Gerencia de Operaciones	3	2	2	2	6	9	MEDIA
IS2	YYY	1	Gerencia de Operaciones	3	2	2	3	7	10	ALTA

“Figura 19: Inventario activos de Información con clasificación”5

3.5 Análisis de Amenazas

Los activos del organismo, tanto de información como de soporte, están expuestos a amenazas, las cuales definimos como: “Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

Para implementar el análisis de amenaza nos basaremos en el catálogo de amenazas propuesto por MAGERIT (Libro 2 “Catálogo de Elementos” - Punto 5), pero fusionando las categorías “Desastres Naturales” y “De origen industrial” en una sola llamada “Del Entorno”. Por lo tanto las amenazas quedan clasificadas en los siguientes bloques:

- Del Entorno [NI]
- Errores y fallos no intencionados [E]
- Ataques intencionados [A]

A continuación se detalla el catálogo de amenazas utilizado:

Tipo	Amenaza	Código	Cod. Magerit
Del Entorno	Fuego	NI1	N1-I1
	Daños por agua	NI2	N2-I2
	Tormenta Eléctrica	NI3	[I.*]
	Terremoto	NI4	[I.*]
	Fluctuaciones/Sobrecarga Eléctrica	NI5	[I.*]
	Explosiones	NI6	[I.*]
	Derrumbes	NI7	[I.*]

	Contaminación mecánica	NI8	[I.3]
	Contaminación electromagnética	NI9	[I.4]
	Avería de Origen Físico o lógico	NI10	[I.5]
	Corte Suministro Eléctrico	NI11	[I.6]
	Condiciones inadecuadas de temperatura o humedad	NI12	[I.7]
	Fallo de servicios de comunicaciones	NI13	[I.8]
	Interrupción de otros servicios y suministros esenciales	NI14	[I.9]
	Degradación de los soportes de almacenamiento de la información	NI15	[I.10]
	Emanaciones electromagnéticas	NI16	[I.11]
Errores y fallos no intencionados	Errores de los usuarios	E1	[E.1]
	Errores del administrador	E2	[E.2]
	Errores del monitorización	E3	[E.3]
	Errores de configuración	E4	[E.4]
	Deficiencias en la organización	E5	[E.7]
	Difusión de software dañino	E6	[E.8]
	Errores de [re-]encaminamiento	E7	[E.9]
	Errores de secuencia	E8	[E.10]
	Escapes de información	E9	[E.14]
	Alteración accidental de información	E10	[E.15]
	Destrucción de información	E11	[E.18]
	Fugas de información	E12	[E.19]
	Vulnerabilidades de los programas (software)	E13	[E.20]
	Errores de mantenimiento / actualización de programas (software)	E14	[E.21]
	Errores de mantenimiento / actualización de equipos (hardware)	E15	[E.23]

	Caída del sistema por agotamiento de recursos	E16	[E.24]
	Pérdida de equipos	E17	[E.25]
	Indisponibilidad del personal	E18	[E.28]
Ataques intencionados	Manipulación de los registros de actividad (log)	A1	[A.3]
	Manipulación de la configuración	A2	[A.4]
	Suplantación de la identidad del usuario	A3	[A.5]
	Abuso de privilegios de acceso	A4	[A.6]
	Uso no previsto	A5	[A.7]
	Difusión de software dañino	A6	[A.8]
	[Re-]encaminamiento de mensajes	A7	[A.9]
	Alteración de secuencia	A8	[A.10]
	Acceso no autorizado	A9	[A.11]
	Análisis de tráfico	A10	[A.12]
	Repudio	A11	[A.13]
	Interceptación de información (escucha)	A12	[A.14]
	Modificación deliberada de la información	A13	[A.15]
	Destrucción de información	A14	[A.18]
	Divulgación de información	A15	[A.19]
	Manipulación de programas	A16	[A.22]
	Manipulación de los equipos	A17	[A.23]
	Denegación de servicio	A18	[A.24]
	Robo	A19	[A.25]
	Ataque destructivo	A20	[A.26]
	Ocupación enemiga	A21	[A.27]
	Indisponibilidad del personal	A22	[A.28]

	Extorsión	A23	[A.29]
	Ingeniería social (picaresca)	A24	[A.30]

"Figura 20: Catálogo de Amenazas implementado"

Frecuencia	Nivel	Descripción
MA	MUY ALTA	Eventos que ocurren con frecuencia diaria o menor
A	ALTA	Eventos que ocurren con una frecuencia mensual
M	MEDIA	Eventos que ocurren cada 6 meses
B	BAJA	Eventos de ocurrencia anual
MB	MUY BAJA	Eventos que ocurren cada 5 o más años

"Figura 21: Tipificación de frecuencias de amenazas"

Luego de identificar las amenazas que pueden afectar nuestros activos, se realizará una valoración las características de cada uno para determinar la Probabilidad. Entendiendo por probabilidad es cuan probable o improbable es la materialización de la amenaza.

Se ha incluido la etapa de Análisis de Controles dentro del análisis de amenazas, para tener una visión del impacto de los controles sobre las probabilidades de cada amenaza sobre los activos del organismo. Se evalúa el grado de implementación de los controles, donde se tiene en cuenta si están implementados controles técnicos, controles organizativos y el grado de supervisión sobre ambos.

El grado de implementación de los controles o salvaguardas sobre los activos, los cuales reducen las probabilidades de que las amenazas se materialicen, se evalúa de acuerdo a la siguiente escala:

Valor	Nivel	Descripción
1	NO IMPLEMENTADO	No se ha implementado ningún control que mitigue la vulnerabilidad.
0.75	EN IMPLEMENTACION	Se ha iniciado la implementación del control.
0.50	IMPLEMENTACIÓN PARCIAL	Existe un control implementado, sin embargo aun puede perfeccionarse.
0.25	IMPLEMENTACIÓN TOTAL	EL control esta implementado en un nivel optimo, y su supervisión es la adecuada.

"Figura 22: Grado implementación Controles"

La evaluación sobre los controles se realiza en forma individual para cada amenaza, tomando los activos o grupos de activos sobre los que actúa. Luego se procede a calcular una "Probabilidad" que resulta de multiplicar la "Frecuencia" de la amenaza por el "Grado de Implementación" de los controles.

Probabilidad = Frecuencia x Grado de Impl. Controles

3.6 Impacto Potencial y Cálculo del Riesgo

Habiendo calculado la Probabilidad debemos ahora determinar impacto de las amenazas en nuestros activos. Para eso realizaremos el Análisis del Impacto, esto es calcular las consecuencias que tendría la materialización de una amenaza sobre el activo, la degradación, teniendo en cuenta el valor del mismo estimado en la clasificación.

Para este análisis utilizaremos la degradación total de la amenaza sobre un activo o grupo de activos, entendiendo por esto el valor más alto de afectación sobre cualquiera de las dimensiones de la información de ese activo y las consecuencias que tendría cada una de las amenazas en caso de materializarse sobre el activo.

Los factores a tener en cuenta en el concepto de degradación son los siguientes:

- La información ha sido visualizada por personas que no tienen permisos para ello. Se produce una pérdida de Confidencialidad.
- La información ha sido modificada sin aprobación. La información sufre una pérdida de Integridad.
- Interrupción del Sistema. No existe posibilidad de acceder a la información. Existe una pérdida de Disponibilidad.
- Destrucción / Pérdida. Parte o toda la información se ha perdido.
- El sistema sigue funcionando con alguna limitación.
- El sistema se interrumpe con consecuencias limitadas.
- Interrupción del sistema con consecuencias severas.

El grado de afectación se medirá en porcentaje, y de acuerdo a la siguiente escala

Valor	Nivel	Descripción
0 %	NULO	La materialización de la amenaza no tiene impacto en el activo, o su impacto es insignificante. Funcionamiento normal.
25 %	BAJO	Se registran pérdidas menores en alguna dimensión, o interrupciones no significativas.
50 %	MEDIO	Afecta a más de una dimensión del activo, o sólo a una pero de manera grave. Se afecta la operatividad del organismo de manera intermedia.
75 %	ALTO	La materialización de la amenaza provoca la pérdida total de una o más dimensiones de la información y/o la interrupción del sistema.

100 %	MUY ALTO	La materialización de la amenaza provoca la perdida de activos o interrupción de procesos críticos de la organización.

"Figura 23: Porcentaje degradación activos"

Con la degradación ya determinada, vamos a proceder a tomar el valor del activo de acuerdo con el cálculo que realizamos en la clasificación de activos (campo Valoración), donde recordemos se tomó en cuenta no solo su criticidad, sino también el tipo de proceso al que da soporte el activo. Con estos 2 valores vamos a calcular el impacto de activo de acuerdo con la fórmula.

Impacto = Degradación x Valor

Una vez que tenemos el valor del impacto podemos iniciar la **Determinación del Riesgo**, la cual se realizará utilizando el impacto y la probabilidad de acuerdo a la fórmula

Riesgo = Impacto x Probabilidad

3.7 Nivel de Riesgo Aceptable y Riesgo Residual

Sabiendo que el análisis realizado ya contempla los controles implementados por el organismo, siendo entonces un análisis de Riesgo Residual, se fijará un **Nivel de Riesgo Aceptable** acorde con esta premisa, y que en principio es más exigente con el nivel de riesgo permitido.

Por ejemplo, de acuerdo a lo decidido por el Comité de Tecnología y Seguridad de la Información y Comunicaciones el nivel de riesgo medio aceptable se fija en **Medio**, lo cual equivale a valores de riesgo iguales o mayores a **14** de acuerdo con la siguiente tabla.

Valor	RIESGO	
1 al 6	Muy Bajo	
7 al 13	Bajo	
14 al 20	Medio	
21 al 27	Medio Alto	
28 al 34	Alto	

"Figura 24: Niveles de Riesgo"

Los riesgos que se encuentren por debajo de este valor, se consideran aceptables y no deben ser tratados.