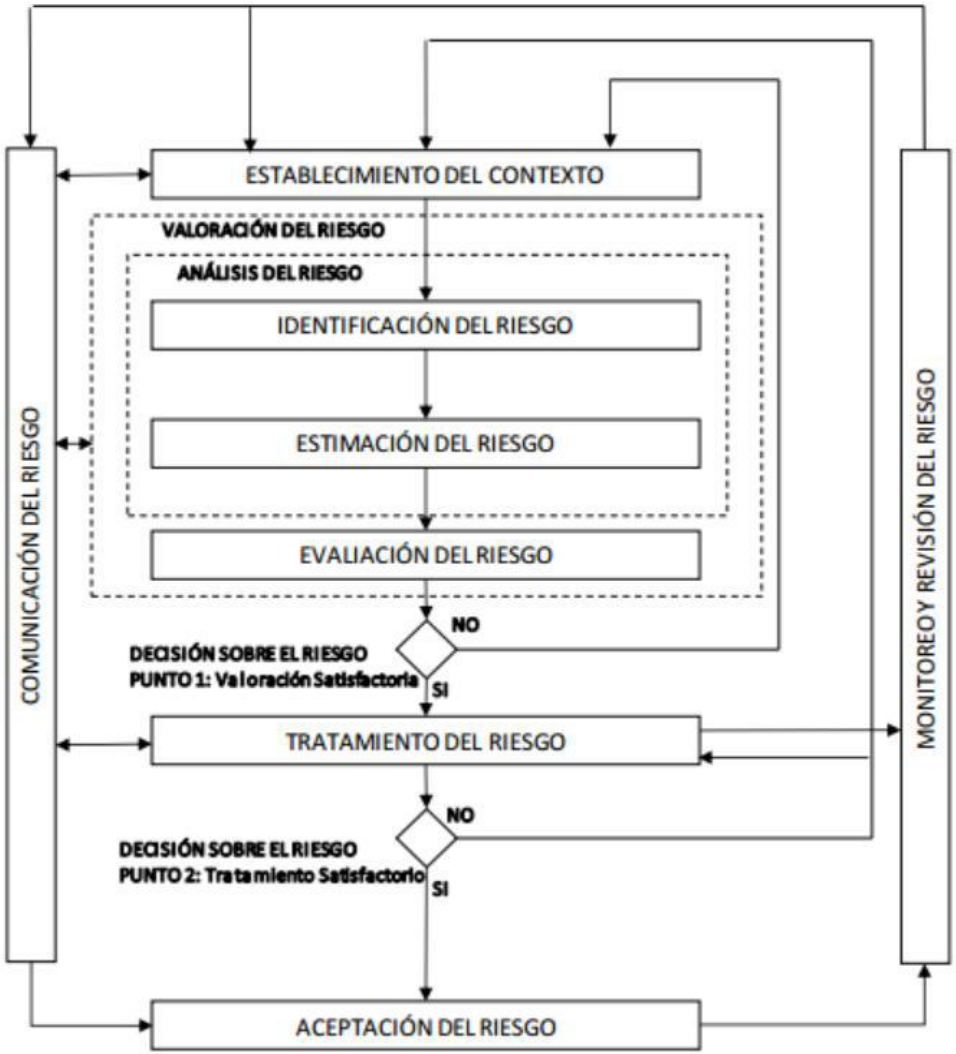
PLAN DE IMPLEMENTACIÓN DE UN SGSI BASADO EN LA NORMA ISO 27001:2013 EN EL ÁMBITO DE LA ADMINISTRACIÓN PUBLICA ARGENTINA

Metodología de Gestión del Riesgo

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 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**.


ESTABLECIMIENTO DEL CONTEXTO
VALORACIÓN DEL RIESGO
ANÁLISIS DEL RIESGO
IDENTIFICACIÓN DEL RIESGO
ESTIMACIÓN DEL RIESGO
EVALIACIÓN DEL RIESGO
NO
DECISIÓN SOBRE EL RIESGO
PUNTO 1: Valoración Satisfactoria
SI
TRATAMIENTO DEL RIESGO
NO
DECISIÓN SOBRE EL RIESGO
PUNTO 2: Tratamiento Satisfactorio
SI
ACEPTACIÓN DEL RIESGO
COMUNICACIÓN DEL RIESGO
MONITOREO Y REVISIÓN DEL RIESGO

Identificación del Riesgo

IDENTIFICACIÓN DE ACTIVOS

El primer paso es realizar el *inventario de activos de información*.

- **Activo de información/primarios:** sistema de información o aplicación informática utilizada para generar o manipular información del organismo. No se tiene en cuenta los activos ***externos***.

- **Activos de soporte:** 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.

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

Inventario de Activos

A los activos se les asignarán un **subtipo**:

Subtipos Activos de Información			
Prioridad	**Nombre**		**Descripción**
3	**SUSTANTIVO**	**IS**	Permiten el cumplimiento de los objetivos fundamentales de la organización
2	**CONDUCCIÓN**	**IC**	Dan sostén operativo para el cumplimiento de los procesos sustantivos.
1	**APOYO**	**IA**	Organizan y facilitan la coordinación de los procesos de la organización
0	**EXTERNO**	**IE**	Procesos cuya administración no es llevada a cabo por el organismo

Valoración = Prioridad + Valor Criticidad

Subtipos Activos de Soporte		
Nombre		**Descripción**
HARDWARE	**HW**	Equipos electrónicos que soportan los servicios prestados
SOFTWARE	**SW**	Componentes lógicos que contribuyen al procesamiento de la información.
INFRAESTRUCTURA	**IF**	Instalaciones físicas y equipamiento que brinda soporte a los activos de hardware.
REDES-COMUNICACIONES	**RC**	Servicios de comunicaciones propios y contratados para transportar información.
CONTENEDOR DE DATOS	**CD**	Dispositivos físicos o lógicos que permiten almacenar información.
PERSONAL	**PS**	Grupos de Personas relacionados con los sistemas de información.
SERVICIOS	**SV**	Servicios contratados a un proveedor externo, exceptuando al tipo RC.

Valoración = heredan la valoración del activo de nivel superior

Inventario de Activos

Para los **Activos de Información** se deben definir los siguientes datos:

- Categoría: Tipo del activo.
- Identificación: Código alfanumérico de identificación única (Categ+Num).
- Nombre Activo: Identificación formal del activo para el organismo.
- 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.
- 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.

Inventario de Activos

Para los A**ctivos de Soporte** se deben definir los siguientes datos:

- Categoría
- Identificación: Código alfanumérico de identificación única (Categ+Num).
- Nombre Activo: Identificación del activo para el organismo.
- Activo de Información Relacionado
- Propietario
- Valoración
- Criticidad

CLASIFICACIÓN DE ACTIVOS

Se realizará en base a: **Confidencialidad** (C), **Integridad** (I) y **Disponibilidad** (D).

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.

Se identificará el tipo de proceso al que están asociados, siendo los valores de esta clasificación **Sustantivo**, **Conducción** y **Apoyo**.

El resultado de estas dimensiones nos dará una **valoración** del activo en función de la **criticidad**.

CONFIDENCIALIDAD

La información contenida por el activo es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Valor	Nivel	Descripción
0	**USO PÚBLICO**	Puede ser conocida y utilizada sin autorización por cualquier persona, sea empleada del organismo o no.
1	**USO RESERVADO-INTERNO**	Puede ser conocida y utilizada por todos los empleados y entidades externas autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves
2	**USO CONFIDENCIAL**	Sólo puede ser conocida y utilizada por un grupo de empleados para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas
3	**USO SECRETO**	Sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves

INTEGRIDAD *La información del activo no ha sido modificada de manera no autorizada.*		
Valor	**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
2	**MEDIO**	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas
3	**ALTO**	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al organismo

DISPONIBILIDAD *Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados, toda vez que lo requieran.*		
Valor	**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
2	**MEDIO**	Información cuya inaccesibilidad permanente durante dos días podría ocasionar pérdidas significativas al organismo
3	**ALTO**	Información cuya inaccesibilidad permanente durante seis horas podría ocasionar pérdidas significativas al organismo

CRITICIDAD		
Valor Criticidad	**Nivel**	**Descripción**
De 0 a 3	**Baja**	Interviene en procesos no directamente relacionados al negocio, aunque son necesarios. Su indisponibilidad causa algún contratiempo pero no afecta la continuidad del negocio.
De 4 a 6	**Media**	Interviene en procesos de apoyo a la organización. Su indisponibilidad puede retrasar un proceso, pero no afecta la continuidad de negocio
De 7 a 9	**Alta**	Interviene en procesos clave para la organización (son necesarios y suficientes). Se pone en peligro la continuidad del negocio, o contiene información con implicaciones legales

IDENTIFICACIÓN DE AMENAZAS

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)

Las amenazas quedan clasificadas en los siguientes bloques:

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

Luego se realizará una valoración las características de cada uno para determinar la **Frecuencia** (cuan probable o improbable es la materialización de la amenaza)

Análisis de amenazas

Frecuencia Numérica			
Nivel		Valor	Frecuencia
MB (5 Años)	MUY BAJA	1	Cada 5 años o más
B (Anual)	BAJA	2	Anual
M (6 Meses)	MEDIA	3	Cada 6 meses
A (Mensual)	ALTA	4	Mensual
MA (Diaria)	MUY ALTA	5	Diaria o menor

ANÁLISIS DE CONTROLES

Con este paso se 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.

Controles Implementados		
Nivel	**Valor**	**Descripción**
No Implementado	1	Ningún control implementado
En Implementación	0.75	Se ha iniciado la implementación
Impl. Parcial	0.5	Existe un control implementado, puede perfeccionarse
Impl. Total	0.25	Control y supervisión implementados a nivel óptimo

La evaluación sobre los controles se realiza en forma individual para cada amenaza, tomando los activos o grupos de activos sobre los que actúa.

Probabilidad = Frecuencia x Grado de Impl. Controles

Estimación del Riesgo

El riesgo es una función del impacto y la probabilidad de ocurrencia de una amenaza.

Análisis del Impacto: consecuencias que tendría la materialización de una amenaza sobre el activo, la **degradación**, teniendo en cuenta el valor del mismo estimado en la clasificación.

Degradación: valor más alto de afectación sobre cualquiera de las dimensiones de la información de ese activo.

DEGRADACION		
Valor	**Nivel**	**Descripción**
0	**NULO**	La materialización de la amenaza no tiene impacto en el activo, o su impacto es insignificante. Funcionamiento normal.
0.25	BAJO	Se registran pérdidas menores en alguna dimensión, o interrupciones no significativas
0.5	**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.
1	**MUY ALTO**	La materialización de la amenaza provoca la perdida de activos o interrupción de procesos críticos de la organización.

Con la determinación de la degradación y el valor de activo se puede calcular el Impacto.

Impacto = Degradación x Valor

Una vez que tenemos el valor del impacto podemos iniciar la Determinación del Riesgo.

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

Evaluación del Riesgo

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: se designa como propietario de todos los riesgos al "Comité de Tecnología y Seguridad de la Información y Comunicaciones" (CoTySIC).

Nivel de Riesgo Aceptable: es el punto a partir del cual se debe proceder a realizar el tratamiento del riesgo.

NIVELES DE RIESGOS

Min. Valor	Max. Valor	RIESGO	
1	7	Muy Bajo	
8	13	Bajo	
14	20	Medio	
21	32	Medio Alto	
33	50	Alto	

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

Tratamiento de Riesgos

Son tratados los riesgos que se encuentran por arriba del nivel aceptable, eligiendo entre una de las siguientes 4 opciones:

MITIGARLO

Implantar los controles necesarios con el fin de que el nivel de riesgo disminuya a un punto que se encuentre bajo el límite aceptable

TRANSFERIRLO

Traspasar a terceros el riesgo con el fin que sean éstos quienes puedan reducir su impacto o gestionar el riesgo de mejor manera.

Tomar acciones tendientes a impedir que el riesgo se vuelva una realidad. Sustituyendo el activo o dejar continuar la actividad relacionada con el activo.

EVITARLO

No realizar ninguna acción que permita evitar que se produzca el riesgo. Cuando no es posible ejecutar ninguna de las otras acciones y la probabilidad es baja o medio-baja.

ACEPTARLO