FASE 4 PLANIFICACIÓN DEL SGSI

FASE 4 Planificación del SGSI

INVENTARIO DE ACTIVOS

En primer lugar necesitamos identificar los activos de información junto con sus amenazas y vulnerabilidades tal como vimos en la sección de DEFINICION DEL ALCANCE

En primer lugar daremos unas pautas para identificar los activos de información

1.- Identifique los servicios tanto internos como externos de la organización

2.- ¿Qué información necesita para desarrollar los servicios?

3.- ¿Qué infraestructura está involucrada en la prestación de los servicios?

Hardware, por ejemplo, computadoras portátiles, servidores, impresoras, pero también teléfonos móviles o memorias USB.

Infraestructura: oficinas, electricidad, aire acondicionado etc.

4.- ¿Aplicaciones Software están involucradas en la prestación de los servicios? No solo el software comprado, sino también el software gratuito.

5.- Identifique las actividades subcontratadas

Servicios legales

Servicios de limpieza

Servicios en la nube

Servicios de correo

Etc.

6.- Identifique las personas de las que dependen los servicios. Considere que tipo de información relevante para el negocio se puede encontrar solo en “las cabezas” de ciertas personas y que a menudo no está disponible en otras formas.

7.- Determine los medios por los que se transmite la información

8.-Identifique los soportes en los que se encuentra la información: no solo en soportes electrónicos como bases de datos, archivos en PDF, Word, Excel y otros formatos, sino también en papel y otras formas.

A continuación les dejamos una recomendación para el tipo de Información y estructura para un

inventario de Activos de acuerdo a la norma **ISO 27001**

Nombre del Proceso

Dueño o propietario del proceso

Nombre del Activo

Descripción del Activo

Tipo de activo de información / Medio

Copia impresa, archivo electrónico: (especificar tipo)

Medio / dispositivo extraíble : (especificar tipo)

¿Contiene Datos personales?

¿Contiene Datos personales Sensibles?

Confidencialidad (Alta – Media – Baja)

Disponibilidad (Alta – Media – Baja)

Integridad (Alta – Media – Baja)

¿Quién custodia el Activo? (si no es funcional)

Periodo de retención de datos

Nivel de protección Actual

Ejemplo:

Para copia impresa:

• Guardado en caja fuerte a prueba de fuego

• Guardado bajo llave en todo momento

• Se mantiene bajo llave durante la noche

• Guardado en armario / archivo sin llave

• Guardado en el escritorio

Para copia electrónica:

• Almacenado en unidades locales – PC portátil sin protección

• Almacenado en unidades locales – PC portátil, el archivo está protegido con contraseña

• Almacenado en la unidad de red en

portátil sin protección
• Almacenado en la unidad de red – PC portátil, el archivo está protegido con contraseña
• Almacenado en PC desprotegido
• Almacenado en la PC, el archivo está protegido con contraseña
• Almacenado en computadora portátil cifrado o PC

NOTA; Si la información se transmite detallar el lugar de destino y al nivel de protección en el lugar de destino

Valoración de Activos y asignación de riesgos

El siguiente paso será asignar a cada activo una valoración del riesgo para cada activo en relación al impacto que tendría una pérdida de confidencialidad, disponibilidad o integridad. En este sentido un riesgo puede definirse como un evento posible con un impacto comercial negativo.

Junto con el impacto deberemos precisar con la mayor exactitud posible la probabilidad de que ocurra dicho evento ya que no basta con el impacto posible ya que el número de ocurrencias esperado es lo que junto al impacto determina finalmente el perfil del riesgo de cada activo.

Entonces, determinar el posible daño es el primer paso. Para ello podríamos definir una escala a aplicar para cada activo en relación a las tres dimensiones de cada información, es

decir cómo afecta su pérdida de confidencialidad, integridad o disponibilidad.

Veamos la siguiente escala de 5 valores

5 puntos impacto Extremo

Cuando existe la posibilidad de que el impacto tenga como consecuencia cualquiera de las siguientes eventos

- Pérdida financiera insoportable para el negocio
- Cobertura de medios negativa internacional a largo plazo; pérdida total de la cuota de mercado
- Enfrentar juicios con posibilidad de encarcelamiento de directivos
- Multas importantes
- Litigios que incluyen acciones colectivas,
- Lesiones o muertes a empleados o terceros, como clientes o vendedores
- Fuga de talentos con consecuencias lesivas para el negocio

4 puntos impacto Importante

Si concurren alguna de las siguientes consecuencias:

- Pérdida financiera entre un valor 1 y un valor 2
- Impacto nacional negativo a nivel de medios de comunicación a largo plazo
- Pérdida significativa de cuota de mercado
- Requisito de comunicación a las entidades reguladoras por incidentes con

un proyecto importante como acción correctiva

Se requiere atención hospitalaria limitada para empleados o terceros, como clientes o vendedores

Alta rotación de personal experimentado

3 puntos impacto Moderado

Pérdida financiera entre un valor 1 y un valor 2

Impacto en medios de comunicación negativo a nivel nacional a corto plazo

Requisito de comunicación a las entidades reguladoras por incidentes con una acción correctiva inmediata

Tratamiento médico ambulatorio requerido para empleados o terceros, clientes o proveedores

Problemas generales en el ánimo o moral del personal y alta rotación

2 puntos impacto Menor

Pérdida financiera entre un valor 1 y un valor 2

Daño reputaciones local

Incidente denunciable al regulador, sin seguimiento

Sin lesiones menores a empleados o terceros, como clientes o proveedores

Problemas generales en el ánimo o moral del personal y aumento en la rotación

1 punto impacto incidental

Pérdida financiera insignificante

La atención de los medios locales se remedia rápidamente

Incidente no reportable a las entidades reguladoras

No hay lesiones para los empleados o terceros, como clientes o proveedores

Insatisfacción del personal

Valoración del impacto en un activo

Teniendo en cuenta la siguiente escala, cada activo tendrá una valoración de 0 a 5 para todas sus dimensiones

0 No Aplicable

1 Incidental

2 Menor

3 Moderado

4 Importante

5 Extremo

ACTIVOX	Confidencialidad	Integridad	Disponibilidad	Nivel Impacto TOTAL
Impacto	0 No Aplica	3 Moderado	4 Importante	7

Con este esquema podremos evaluar el nivel de impacto del riesgo para la seguridad de la información de todos y cada uno de los activos

El siguiente paso consiste en elaborar un catálogo de amenazas considerando como tales a cualquier intento o evento capaz de alterar la seguridad de la información:

CATÁLOGO DE AMENAZAS

Para encontrar las amenazas que pueden afectar a una organización en concreto, se

deben conocer las fuentes de amenazas y las áreas específicas del sistema que pueden verse afectadas así como los activos de seguridad de la información que se pueden proteger por adelantado.

Para comprender e identificar las amenazas y sus posibles impactos contamos con diferentes maneras para clasificar dichas amenazas así como los criterios. Normalmente deberíamos tener en cuenta para ello la fuente de la amenaza, los agentes y las motivaciones.

Otra forma de resolver esta cuestión seria considerar las amenazas bajo el prisma del impacto que pueden causar en la seguridad de la información

Aquí les proponemos identificar primero las amenazas para en un segundo paso analizar el nivel de impacto de cada una aplicada cada activo de información

Existen numerosos catálogos de amenazas, a modo de ejemplo les proponemos un catálogo genérico

Ejemplo de catálogo de amenazas para la seguridad de la información:

CASO PRACTICO: catálogo de amenazas para la seguridad de la información

• A1 Fuego

Aquí podríamos distinguir sobre fuego en CPD (centro proceso de datos) o en oficinas etc.

• A2 Condiciones climáticas desfavorables

Se trata de analizar las consecuencias para equipos e instalaciones en caso de condiciones adversas. Como ejemplo podríamos evaluar las consecuencias de las altas temperaturas en verano junto con las necesidades de los equipos de climatización. En este caso deberíamos evaluar fallos en equipos por altas temperaturas o desmagnetizaciones de soportes de información etc.

• A3 Inundaciones

Aquí deberíamos evaluar las posibles causas de inundaciones de agua en las instalaciones y oficinas

Inundaciones por interrupciones de suministro

Sistemas de riego

Sistemas de calefacción

Sistemas contra incendios

Sabotajes (grifos bloqueo de desagües etc.)

• A4 Contaminación, polvo, corrosión

En este punto podríamos tener en cuenta el riesgo de contaminación de salas de

equipos especialmente sensibles a niveles de polvo o sustancias en suspensión etc.

- Contaminación por obras o reformas en las salas
- Polvo derivado de tareas de empaquetado
- Instalaciones de nuevos equipos

• A5 Desastres Naturales

Probabilidad de ser afectado por inundaciones, terremotos, tormentas eléctricas, impactos sobre la disponibilidad de servicios de comunicaciones etc.

• A6 Desastres ambientales

Probabilidad de ser afectado por desastres ambientales

- Incendios
- Explosiones
- Fugas
- Evaluación del entorno (empresas vecinas con actividades peligrosas)
- Interrupción de accesos al trabajo

• A7 eventos importantes en el medio ambiente

Probabilidad de ser afectado por obras realizadas en el entorno, manifestaciones o desordenes públicos etc.

• A8 Interrupción de la fuente de alimentación

- Probabilidad de interrupciones micro cortes en el suministro eléctrico<

Estabilidad de la red

Subidas de tensión

Afectaciones a sistemas de seguridad, ascensores

Interrupciones prolongadas

- **A9 Interrupción de las redes de comunicación**

Como afectan las interrupciones de las comunicaciones a

Comunicación con los clientes

Procesos propios del negocio

Perdidas de datos

Procesos de pedidos

Dependencia de servicios de Internet

Etc.

- **A10 Interrupción del suministro de red**

Sistemas o tareas afectadas por falta de suministro

Climatización o ventilación

Agua y alcantarillado, (Sistema contra incendios)

Gas

Sistemas de alarma y control (por ejemplo, para robo, incendio, control de limpieza)

Sistemas de comunicación internos

- **A11 Fracaso o interrupción de los proveedores de servicios**

Interrupciones parciales o totales de servicios subcontratados

Niveles de calidad de los servicios no aceptables

Indisponibilidad de instalaciones externas

• A12 Interferencias

Interferencias en servicios inalámbricos (p. ej. Redes WLAN, Bluetooth, GSM, UMTS)

• A13 Emisiones comprometidas

Riesgo de interceptación de información confidencial por radiaciones emitidas por equipos

• A14 Espionaje

Riesgo de exposición de información sobre la compañía, productos y servicios que puedan ser utilizados por la competencia o entidades para perjuicio de la actividad de la organización

Escuchas ilegales

Intercepción de señales de transmisión

Intercepción de transmisiones desprotegidas de datos en redes publicas

• A15 Robo de dispositivos, soportes de almacenamiento y documentos

Robo de soportes de almacenamiento de datos, sistemas de TI, accesorios, software o datos de clientes etc.

• A16 Pérdida de dispositivos, soportes de almacenamiento y documentos

Pérdidas de equipos portátiles o soportes de almacenamiento de datos (Tarjetas de memoria) Documentos impresos olvidados en restaurantes o en lugares públicos, medios de transporte

- **A17 Mala planificación o falta de adaptación**

  Procedimientos inadecuados de mantenimiento

  Protocolos de transferencia

  Procesos de adquisición de nuevas tecnologías

- **A19 Divulgación de información sensible**

  Accesos no autorizados

  Reciclaje de equipos y soportes

  Destrucción de equipos y soportes

  Software malicioso

  Difusión de información inadvertida en procesos externos (Ordenes de reparación etc.)

  Robo de contraseñas

  Etc.

- **A18 Información o productos de una fuente no confiable**

  Verificación insuficiente de información o software externo

  Apertura de archivos o aplicaciones provenientes de fuentes no verificadas en equipos de trabajo (P. ej. emails)

Instalación de aplicaciones y actualizaciones de software por usuarios finales

- **A19 Manipulación de hardware o software**

  Venganzas de empleados

  Actuaciones ilícitas para beneficio propio

- **A20 Manipulación de información**

  Datos falos en formato electrónico o en papel

  Falsificación o modificación de datos y documentos

- **A21 Acceso no autorizado a los sistemas de TI** Accesos no autorizados a aplicaciones o sistemas

- **A22 Destrucción de dispositivos o soportes de almacenamiento**

Destrucción de soportes de almacenamiento o sistemas TI por venganzas, negligencias o usos indebidos

- **A23 Fallo de dispositivos o sistemas**

  Fallos en dispositivos críticos del sistema

  Fallos técnicos por mal funcionamiento

  Fallos por uso indebido o errores humanos

  Fallos por causas externas (falta de suministro etc.)

Fallos por sabotaje

Fallos por accidentes

- **A24 Mal funcionamiento de dispositivos o sistemas**

  Por fatiga o desgaste del material

  Falta de mantenimiento

  Tolerancias de fabricación

  Errores de diseño

  Superación de límites máximos de carga o condiciones de uso

- **A25 Falta de recursos**

  Congestiones en el servicio (cuellos de botella)

  Sobrecargas en sistemas e infraestructuras

  Requisitos de nuevas aplicaciones que exceden las capacidades existentes

  Falta de recursos económicos

- **A26 Vulnerabilidades o errores del software**

  Errores de programación

  Fallos en navegadores y aplicaciones WEB

- **A27 Violación de leyes o regulaciones**

  Violaciones de leyes sobre procesamientos de información

  Incumplimientos de cláusulas contractuales

Incumplimientos legales en el tratamiento de datos personales

- **A28 Uso no autorizado o administración de dispositivos y sistemas**

- **A29 Uso incorrecto o administración de dispositivos y sistemas**

- **A30 Abuso de Autorizaciones**

- **A31 Ausencia de personal**

  Bajas prolongadas

  Sustituciones por bajas o vacaciones

  Bajas masivas por epidemias

- **A32 Terrorismo**

  Ataques con explosivos

  Incendios premeditados

  Ataques con armas de fuego

- **A33 Coerción, extorsión o corrupción**

Uso indebido de datos o acceso a datos confidenciales por chantajes, extorsiones o corrupción de personas

- **A34 Robo de identidad**

  Robos de datos personales para suplantar identidades (datos bancarios etc.)

  Ataques con datos ficticios (Suplantación de identidades por

maquinas o robots)

• A35 Comportamientos anti-éticos

Negación de recepción de informaciones, mensajes o instrucciones de seguridad (p. ej. negar la recepción de emails o pedidos realizados etc.)

• A36 Abuso de datos personales

Violaciones a las leyes sobre protección de datos

Recoger datos sin base legal o consentimiento,

usa para fines diferentes al objetivo establecido en el momento de la recolección,

eliminación de datos personales demasiado tarde

Divulga datos de forma no autorizada

Etc.

• A37 Software malicioso

Ataques de software malicioso tales como virus, gusanos y caballos de Troya.

• A38 Ataques DoS o denegación de servicio

Interrupciones de los procesos comerciales (envió masivo de formularios etc.)

Daños a la infraestructura (Bloque de accesos etc.)

Fallos por sobrecarga por ataques por accesos masivos provocados

• A39 Ingeniería Social

Los ataques típicos de ingeniería social para acceder de forma no autorizada suponen casi siempre una suplantación de identidad basándose en la confianza, miedo o respeto de personas. Normalmente se utilizan llamadas urgentes para reclamar información de contraseñas etc. amparados en la autoridad, la amistad o la confianza.

• A41 Reproducción de mensajes

Intercepción de transmisiones para introducir datos maliciosos y retransmitir el mensaje

• A42 Entrada no autorizada a las instalaciones

• A43 pérdida de datos

Perdida de la disponibilidad de datos por borrados indebidos o corrupción por Software malicioso, usos indebidos o fallos técnicos

VALORACIÓN DE LAS AMENAZAS PARA LA SEGURIDAD DE LA INFORMACIÓN

FRECUENCIA O PROBABILIDAD DE OCURRENCIA

Para cada amenaza deberemos identificar la probabilidad de que ocurra o la frecuencia con la que puede presentarse determinando en una escala su valor.

La escala para definir la frecuencia podría ser:

Probabilidad Mínima o muy baja:
No se identifican agresores o incidentes ni hay antecedentes (valor 0)

Probabilidad Potencial o Baja:
Se identifica historial de este tipo de agresiones así como incidentes dentro del sector o área geográfica, pero no hay incidentes registrados en nuestra organización. Se esperan posibles incidentes de forma esporádica (Valor 1)

Probabilidad Creíble o Media:
Se identifica historial de este tipo de agresiones así como incidentes en nuestra organización. Se esperan posibles incidentes de forma periódica sin frecuencia determinada. (Valor 2)

Probabilidad Definida o Alta:
Se identifica historial de este tipo de agresiones e incidentes en nuestra organización identificándose el origen. Incidentes o eventos de esta naturaleza ocurren con frecuencia conocidos (Valor 3)

NIVEL DE VULNERABILIDAD

La vulnerabilidad considera el impacto potencial de la perdida de información si la amenaza se

produce. Se trata de considerar en qué grado la organización se ve afectada cuando la amenaza se realiza.

Un componente clave de la evaluación de la vulnerabilidad es definir adecuadamente las calificaciones para el impacto de la pérdida y la vulnerabilidad ya que esto puede variar para distintos activos.

No es lo mismo la indisponibilidad de datos de varios minutos en un sistema de control de tráfico ferroviario que en la indisponibilidad de minutos de la base de datos de empleados de la misma organización.

Ejemplo de escala de valoración de vulnerabilidades de una amenaza determinada

Menor deterioro inexistente (Valor 0):
No hay impacto en las instalaciones ni en las operaciones. La interrupción es menor a 2 horas. No hay pérdida ni daño en activos importantes.

Perceptible o deterioro bajo (Valor 1):
Las instalaciones quedan temporalmente cerrada o no puede operar, pero puede continuar su actividad. La interrupcion es menor a 8 horas. Existe un daño limitado de activos. La mayoría de las instalaciones no se verán afectadas.

Grave o deterioro medio (Valor 2):
Instalaciónes parcialmente dañadas

(climatización, agua, humo, impacto o incendio en algunas áreas etc.).

Algunos activos de información están dañados sin posibilidad de reparación, pero la instalación permanece intacta en su mayoría. Toda la instalación puede estar cerrada por un período de hasta una semana y una parte de la instalación puede estar cerrada por un período prolongado (hasta 4 semanas). Es posible que se deba mover algunos activos a ubicaciones remotas para protegerlos del daño ambiental.

Catastrófica o deterioro alto (Valor 3):
Daños irreparables en instalaciones / afectada más allá del uso habitable. La mayoría de los datos y activos se pierden, destruyen o dañan sin posibilidad de reparación o restauración.

ANÁLISIS DE RIESGOS

Ante una amenaza potencial podemos ahora establecer un análisis en base a los parámetros de la frecuencia y el valor de la vulnerabilidad.

Esto lo haremos en diferentes pasos

PASO 1 DEFINIR NIVELES DE IMPACTO DE LAS AMENAZAS

Cada amenaza tendrá un nivel de impacto en base a su Nivel de Vulnerabilidad que a su vez estará condicionada al nivel asociado a cada dimensión del activo.

Así obtenemos un nivel de impacto asociado a cada dimensión (Confidencialidad, Disponibilidad

e Integridad) del activo

Tabla 1 Valores Impacto						
Valor de Vulnerabilidad de la amenaza	VALORES DE DE LAS DIMENSIONES DE LOS ACTIVOS 0 No Aplicable 1 Incidental 2 Menor 3 Moderado 4 Importante 5 Extremo					
	0	1	2	3	4	5
0 - Deterioro Menor / inexistente	0	0	0	0	0	0
1 - Deterioro Perceptible / Bajo	0	1	2	3	4	5
2 - Deterioro Grave / medio	0	2	3	4	5	6
0 - Deterioro Catastrófico / Alto	0	3	4	5	6	7

Tabla 1 Valores Impacto

PASO 2 CALCULAR LOS VALORES DE IMPACTO DE CADA ACTIVO

Con los datos que ya tenemos

Escala de valoración de amenazas (probabilidad/ocurrencia)

Escala de valoración de activos (Nivel de deterioro /Confidencialidad/Disponibilidad/Integridad)

Podemos entrar en la valoración de activos

Tabla 2 de Valoración de Amenazas de Activos					
	ACTIVOS		0 No Aplicable 1 Incidental 2 Menor 3 Moderado 4 Importante 5 Extremo		
	Sistema de Correo Electrónico	Probabilidad / Ocurrencia 0 Minima - 1 Baja - 2 Media - 3 Alta	Deterioro Confidencialidad	Deterioro Integridad	Deterioro Disponibilidad
AMENAZAS	Fuego	1	0	2	5
	Inundacion	1	0	2	4
	Interrupcion de suministro Eléctrico	2	1	2	4
	Robo de dispositivos	3	3	3	0
	Fallo Comunicaciones	3	3	3	0
	Servidor para la página web corporativa				
AMENAZAS	Fuego	2	0	3	5
	Inundacion	1	0	3	4
	Interrupcion de suministro	3	1	2	3
	Robo de dispositivos	1	3	3	0
	Fallo Comunicaciones	2	3	3	0

Tabla Valoración de activos

PASO 3 CALCULAR NIVEL DE IMPACTO

Basados en la tabla anterior donde tenemos la valoración de los activos en cuanto a su probabilidad y grado de deterioro, podemos calcular el nivel de impacto para cada valor combinado de ambos valores buscando su equivalencia en la tabla tabla 1 Valores de Impactos.

Valor Probabilidad/Ocurrencia & Valor Deterioro = Nivel de impacto

Así obtendremos una tabla como la que sigue.

	Tabla 3 de Nivel de Impacto			
	Niveles de Impacto			
	Sistema de Correo Electrónico	**Impacto Confidencialidad**	**Impacto Integridad**	**Impacto Disponibilidad**
AMENAZAS	Fuego	0	2	5
	Inundacion	0	2	4
	Interrupcion de suministro Electrico	2	3	5
	Robo de dispositivos	5	5	0
	Fallo Comunicaciones	5	5	0
	Servidor para la página web corporativa			
AMENAZAS	Fuego	0	4	6
	Inundacion	0	3	4
	Interrupcion de suministro	3	4	5
	Robo de dispositivos	3	3	0
	Fallo Comunicaciones	4	4	0

Nivel de impacto

PASO 4 CALCULAR RIESGO

Una buena recomendación

El análisis de riesgos debe realizarse sin tener en cuenta las medidas para mitigar o evitar el riesgo que se estén tomando actualmente. Se trata de evaluar el riesgo y su impacto real antes de que se apliquen medidas para

poder evaluar realmente qué medidas son efectivas y necesarias.

El objetivo final es asignar un valor de riesgo para cada activo de información detallado para cada amenaza a la que está expuesta para así poder asignar luego un tratamiento para los riesgos que resulten con niveles altos. Esto lo veremos más adelante.

Ahora en primer lugar tendremos definir nuestra MATRIZ GENERAL DE RIESGOS según los datos que ya tenemos

Para la matriz de riesgos utilizaremos los valores de la Tabla 1 Valores de Impacto a los cuales les asignaremos un valor de Riesgo según la escala de Valores de la probabilidad del riesgo:

Tabla 2 de Valoración de Amenazas de Activos					
	ACTIVOS		0 No Aplicable 1 Incidental 2 Menor 3 Moderado 4 Importante 5 Extremo		
	Sistema de Correo Electrónico	Probabilidad / Ocurrencia 0 Minima - 1 Baja - 2 Media - 3 Alta	Deterioro Confidencialidad	Deterioro Integridad	Deterioro Disponibilidad
AMENAZAS	Fuego	1	0	2	5
	Inundacion	1	0	2	4
	Interrupcion de suministro Eléctrico	2	1	2	4
	Robo de dispositivos	3	3	3	0
	Fallo Comunicaciones	3	3	3	0
	Servidor para la página web corporativa				
AMENAZAS	Fuego	2	0	3	5
	Inundacion	1	0	3	4
	Interrupcion de suministro	3	1	2	3
	Robo de dispositivos	1	3	3	0
	Fallo Comunicaciones	2	3	3	0

Valores de Riesgo

Esta será por tanto nuestra matriz general de riesgos con valores de riesgo de 1 al 9

Vamos ahora a calcular el riesgo para cada activo de información. Para ellos nos tenemos que valer de los datos de las tablas

Tabla 2 de Valoración de Amenazas de Activos

Tabla 3 de Nivel de Impacto

Tabla 4 Valores de Riesgo

Para cada amenaza calcularemos el valor del riesgo buscando en la tabla 2 el valor de la probabilidad de cada amenaza y en la tabla 3 su correspondiente Valor de impacto para determinar su valor de Riesgo correspondiente en la Tabla 4

Valor Probabilidad/Ocurrencia & Nivel de Impacto = Nivel de Riesgo

Con ello obtendríamos una tabla con la valoración del riesgo denominada mapa de riesgos para cada activo y amenaza

Tabla 1 Valores Impacto

Valor de Vulnerabilidad de la amenaza	VALORES DE DE LAS DIMENSIONES DE LOS ACTIVOS 0 No Aplicable 1 Incidental 2 Menor 3 Moderado 4 Importante 5 Extremo					
	0	1	2	3	4	5
0 - Deterioro Menor / inexistente	0	0	0	0	0	0
1 - Deterioro Perceptible / Bajo	0	1	2	3	4	5
2 - Deterioro Grave / medio	0	2	3	4	5	6
0 - Deterioro Catastrófico / Alto	0	3	4	5	6	7

Cálculo de Valores de Impacto

EVALUACIÓN DE RIESGOS

Una vez que tenemos determinado un valor de riesgo para cada amenaza que puede afectar a

un activo de información deberemos en primer lugar definir los criterios aceptables para el riesgo. En otras palabras, tendremos que designar que niveles de riesgos son asumibles y cuales deberemos tomar medidas

Para nuestro caso de ejemplo vamos a definir 4 niveles de riesgo para establecer los criterios de tratamiento o aceptación de riesgos según las puntuaciones posibles que determinamos en la Tabla 4 Valores de Riesgo

CALIFICACION DEL RIESGO	DESCRIPCIÓN
Muy alto (7-9)	El riesgo es totalmente inaceptable. Se deben tomar medidas inmediatas para reducir estos riesgos y mitigar los riesgos.
Alto (5-6)	El riesgo es inaceptable. Las medidas para reducir el riesgo y los riesgos de mitigación deberían implementarse lo antes posible.
Medio (3-4)	El riesgo puede ser aceptable en el corto plazo. Los planes para reducir los riesgos y mitigar los peligros deberían incluirse en los planes y presupuestos futuros.
Bajo (0-2)	Los riesgos son aceptables. Se deben implementar medidas para reducir aún más el riesgo o mitigar los peligros junto con otras mejoras de seguridad y mitigación.

Clasificación y valoración del riesgo

Con base en los hallazgos del análisis de riesgos, el siguiente paso en el proceso es identificar las medidas disminuyan los diversos niveles de riesgo. Estos se denominan dentro de la norma ISO 27001 como controles de riesgos para la seguridad de la información

En primer lugar podríamos considerar realizar un plan urgente para incluir actualizaciones de controles adicionales por encima de los estándares mínimos recomendados por la organización, según sea necesario, para abordar las amenazas específicas y los riesgos inaceptables asociados que se hayan identificado siempre que se hayan evaluado los

costes estimados para implementar dichas las medidas.

TRATAMIENTO DE RIESGOS

Una vez identificados y valorados los riesgos el siguiente proceso dentro de la gestión de riesgos es realizar un plan para el tratamiento de los riesgos identificados.

Los resultados de la evaluación de riesgos nos ponen en primer lugar una selección de los riesgos que no son aceptables para la organización.

El tratamiento de estos riesgos inaceptables es la tarea principal del siguiente paso del tratamiento de riesgo.

La pregunta es: ¿Qué opciones tenemos a la hora de afrontar cada uno de los riesgos inaceptables?

Antes de establecer medidas concretas para mitigar estos riesgos tenemos cuatro opciones de tratamiento de riesgo:

• MITIGAR EL RIESGO

Se trata de disminuir los riesgos hasta un nivel de riesgo aceptable mediante la aplicación de controles de seguridad del Anexo A incluidos en el documento “anexo A de la norma ISO 27001” o también referenciado como ISO 27002

• TRANSFERIR EL RIESGO

Dependiendo del tipo de riesgo podemos pensar en transferir el riesgo. La transferencia de riesgos es una estrategia de gestión y control de riesgos que implica el cambio contractual de un riesgo puro de una parte a otra. Un ejemplo es la compra de una póliza de seguro, por la cual se transfiere un riesgo específico de pérdida del titular de la póliza a la aseguradora.

• EVITAR EL RIESGO

Prevenir o evitar un riesgo mediante la eliminación de peligros, actividades y exposiciones que pueden afectar negativamente los activos de información una organización. NO se trata de una gestión propia de los riesgos que tiene como objetivo controlar los daños y las consecuencias financieras de los eventos amenazantes, la prevención de riesgos busca evitar por completo el compromiso de los eventos.

• ACEPTAR EL RIESGO

Aceptar el riesgo significa que, aunque el riesgo está identificado y registrado en el proceso de gestión de riesgos, no se realizará ninguna acción. Simplemente se acepta que pueda suceder y se aplicara un tratamiento específico si así ocurre.

Esta es una buena estrategia para usar con riesgos muy pequeños: riesgos que no tendrán un gran impacto en la actividad de la organización si llega a ocurrir y existe una

solución fácil en caso de que surja. Esto lo haremos en el caso que el coste de una estrategia alternativa de gestión de riesgos para enfrentar el riesgo sea mayor que los recursos empleados en asumir el riesgo.

RESPONSABLE DEL RIESGO

El siguiente paso será definir qué estrategia se va a seguir para tratar cada uno de los riesgos identificados. En este proceso ha de identificarse al propietario de los riesgos quien deberá intervenir en la toma de decisión del tratamiento que se va a realizar cada una de las amenazas y riesgos identificados

Resumiendo, en en análisis de riesgos tenemos la documentación sobre

- Documentación sobre los criterios utilizados para las valoraciones de los riesgos y las evaluaciones particulares y hemos de generar explicando como hemos valorado los impáctos de cada riesgo y que vimos en capítulos anteriores
- Documentación sobre las valoraciones intrínsecas de cada riesgo
- El inventario de activos de información con la identificación de los propietarios de cada activo
- La definición del riesgo asumible tomada en la evaluación de riesgos

A partir de aquí podemos determinar que vamos a hacer con cada uno de los riesgos y documentarlo explicando la alternativa de

tratamiento de riesgos elegida (Mitigar, Trasladar, Evitar o Asumir el riesgo)

SELECCIÓN DE CONTROLES: DECLARACIÓN DE APLICABILIDAD

La última etapa consiste en identificar los controles de seguridad que vamos a aplicar a los activos que hemos determinado para el tratamiento de mitigación de riesgos.

Para la selección de controles convendría tener un cuadro sobre las características, y clasificación de la información de cada activo para poder seleccionar los controles adecuados

Esta información preferiblemente ya debe ser recogida en el Inventario de activos donde se puede incluir una:

- Clasificación de la información (datos personales, nivel de confidencialidad etc.)
- Necesidad de establecer controles de acceso
- Incluida o no en procesos de copia de seguridad
- Soportes en que se encuentra
- Necesidades transmitir la información etc.

A partir de esta información podremos establecer una serie de controles técnicos y organizativos para proteger el activo de las amenazas.

Finalmente deberemos realizar un análisis de aplicabilidad o Declaración de aplicabilidad tomando en cuenta todos los controles del Anexo A en orden a verificar que no se ha dejado fuera ningún control que se pueda aplicar a la protección de este activo

Obviando los controles obligatorios de la norma ISO 27001 como la asignación de responsabilidades o Política de privacidad, tendremos que realizar y documentar este análisis de aplicabilidad lo que constituirá nuestra declaración de aplicabilidad

Modelo de declaración de aplicabilidad ISO 27001

		Activo 1				
A9	Control de Acceso	Implementado	Aplica a los riesgos del activo	Coste de implementacion Aceptable	Coste de mantenimiento Aceptable	Justificacion o comentarios
9.1.1	Política de control de acceso	SI/NO	SI/NO	SI/NO	SI/NO	
9.1.2	Acceso a las redes y a los servicios de red	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.1	Registro y baja de usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.2	Provisión de acceso de los usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.3	Gestión de privilegios de acceso	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.4	Gestión de la información secreta de autentificación de los usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.5	Revisión de los derechos de acceso de usuario	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.6	Retirada o ajuste de los derechos de acceso	SI/NO	SI/NO	SI/NO	SI/NO	

Modelo de declaración de aplicabilidad ISO 27001