P-02 Gestión de los riesgos y oportunidades.

CONTENIDO

Revisado por:	Aprobado por: Dirección	Elaborado por: Resp. de Sistema
Fecha:	**Fecha:**	**Fecha:**
Firma:	**Firma:**	**Firma:**

0. Objeto

El objetivo de este proceso es el de gestionar los riesgos y oportunidades, que son de aplicación a **CLÍNICA BEIMAN**, estableciendo un marco de trabajo claro, transparente y conocido por toda la organización, que garantice que los riesgos de son identificados y gestionados de forma adecuada y las oportunidades identificadas y priorizadas.

En el presente proceso se definirá la metodología establecida para la identificación, evaluación, análisis, gestión y tratamiento de riesgos y oportunidades.

De forma adicional se establecen los criterios para el análisis, evaluación y prueba de los controles.

0.1. Entradas y salidas del proceso

Entradas:

- Identificación y análisis de nuestro Contexto.
- Tolerancia a riesgos e identificación de oportunidades de nuestra organización
- Necesidad de identificar, evaluar, analizar y someter a tratamiento los riesgos y las oportunidades.
- Evaluar la idoneidad de los controles existentes.
- Identificar, analizar y gestionar las oportunidades de mejora

Salidas:

- Identificación de riesgos (amenazas) y oportunidades
- Análisis y evaluación de riesgos y oportunidades
- Evaluación de los controles
- Plan de Control de Riesgos
- Plan de acción de Oportunidades

1. Enfoque para el análisis de riesgos

En **CLÍNICA BEIMAN** se ha decidido que, para una adecuada gestión de riesgos de seguridad de la información, en cumplimiento de los requisitos de la norma ISO 27001, se aplicará un enfoque que considerará dos análisis complementarios:

- En primer lugar se realizará un análisis de riesgos asociado al contexto de la organización, en el que se considerarán los riesgos y oportunidades relacionados con los diferentes procesos de la organización, y cuyo desarrollo se apoyará en la **IT-0201 Apreciación de Riesgos por Procesos**.

Por otro lado, para dar cumplimiento al requisito de la norma que requiere un análisis de los riesgos asociados a las pérdidas de Confidencialidad, Disponibilidad e Integridad, se realizará un análisis de los riesgos asociados a los activos de información, cuyo desarrollo se apoyará en **la IT-0202 Apreciación de Riesgos por Activos.**

2. Apreciación de riesgos por procesos

Inicialmente se desarrollará un análisis de riesgos asociado a los procesos de la organización, que seguirá las siguientes fases y que se apoyará en la **IT-0201 Apreciación de Riesgos por Procesos**. Este análisis tendrá como base y punto de entrada en análisis de contexto realizado.

2.1. Establecimiento del contexto

CLÍNICA BEIMAN determina las cuestiones externas e internas que son pertinentes para su propósito y su dirección estratégica y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información.

Para ello desde **CLÍNICA BEIMAN** se lleva a cabo un análisis, permanente, de su entorno:

- Externo: Relacionado con aspectos de tipo: Legal, tecnológico, competitivo, de mercado, cultural, social y económico.
- Interno. Relacionado con cuestiones relativas a: los valores, la cultura, los conocimientos y el desempeño de la organización.

CLÍNICA BEIMAN con carácter anual, lleva a cabo la determinación de las cuestiones externas e internas que son pertinentes para su propósito y su dirección estratégica y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la calidad y seguridad de la información, durante la Revisión del Sistema por la Dirección, de acuerdo a lo documentado en el Manual del Sistema.

2.2. Establecimiento del concepto de riesgo

Consideramos “RIESGOS” como efectos de la incertidumbre de los objetivos establecidos en nuestra organización. Los efectos pueden generar impactos positivos, negativos o ambos: los impactos positivos los denominamos ***oportunidades*** y los negativos como ***riesgos***. Ambos pueden provenir de fuentes internas o externas y afectan a la implementación de la estrategia o logro de nuestros objetivos.

2.3. Definición de criterios de aceptación/tolerancia a los riegos

En **CLÍNICA BEIMAN** buscamos reducir todos los riesgos en la medida de lo posible y sometemos a tratamiento todas aquellas conductas, operaciones y/o actividades que obtengan una evaluación de riesgo actual SUPERIOR A BAJO.

2.4. Identificación de riesgos en procesos

Para la identificación de los riesgos en nuestras actividades (Riesgo Operacional) nos basamos en el análisis de los procesos identificados en nuestro contexto. En la identificación de riesgos participan los Responsables de Área, Dirección y el Responsable del Sistema, con el fin de identificar aquellas situaciones, operaciones o actuaciones que pueden suponer un riesgo.

Esta participación se hace mediante reuniones de trabajo en la cuales utilizaremos la "tormenta de ideas". En esta reuniones participa personal de **CLÍNICA BEIMAN** en función de sus responsabilidades, conocimientos y experiencia, en especial la del Responsable del Sistema quien liderará esta actividad. También son consideraciones relevantes a tener en cuenta para la identificación de riesgos las recomendaciones y guías sectoriales sobre riesgos, datos y experiencia de nuestra propia organización (No Conformidades, Auditorías internas y externas, actividad de evaluación de eficacia de los controles, quejas, reclamaciones, investigaciones, satisfacción de clientes y otras partes interesadas, etc.)

En el registro **R-0201 Evaluación de Riesgos por Procesos** se conserva registro de los riesgos identificados en los procesos de nuestra organización. Por su parte, las oportunidades se registran en el **R-0202 Evaluación de oportunidades**.

Esta identificación y las actividades consecuentes se realizarán y revisarán con una periodicidad **mínima ANUAL** o bien en casos de cambios relevantes en el **contexto** de nuestra organización.

2.5. Análisis del riesgo

El Responsable del Sistema analiza los riesgos identificados, siguiendo lo indicado en la metodología definida en la Instrucción de Trabajo (**IT-0201 Apreciación de Riesgos por Procesos**) que describe la sistemática empleada para el análisis y evaluación de los riesgos con el fin de evaluar objetivamente el nivel de **PROBABILIDAD** y la **gravedad** o **IMPACTO** que la materialización el mismo tendría en nuestra organización, todo ello en función a nuestro contexto.

2.6. Análisis y evaluación de la idoneidad de los controles

El Responsable del Sistema analiza y evalúa la idoneidad de los controles existentes que afecten a cada riesgo identificado, en función a su eficacia, para analizar su nivel de vulnerabilidad siguiendo la metodología establecida en la Instrucción de Trabajo (**IT-0201 Apreciación de Riesgos por Procesos**).

2.7. Evaluación del riesgo

Una vez analizado y evaluado el riesgo inherente, así como la idoneidad de los Controles aplicados, completamos la evaluación del riesgo actual. Todo ello según lo descrito en la instrucción técnica de referencia. (**IT-0201 Apreciación de Riesgos por Procesos**).

La evaluación del riesgo actual de cada uno de los riesgos identificados nos permite clasificarlos y priorizarlos obteniendo una visión clara de aquellos riesgos sobre los que tenemos que tomar acciones de gestión, mitigación y tratamiento en función al nivel de tolerancia a riesgos fijado por nuestra organización.

El Responsable del Sistema mantiene registro y evidencia de todas las actividades relacionadas con el análisis y evaluación del riesgo.

El resultado de esta actividad queda reflejado en el registro **R-0201 Evaluación de Riesgos por Procesos**

2.8. Tratamiento de riesgos

En **CLÍNICA BEIMAN** hemos determinado actuar, al menos, sobre todos aquellos riesgos cuya evaluación de riesgo actual haya arrojado un nivel POR ENCIMA DE BAJO. Para tales riesgos se definen planes de acción con el objetivo de mitigarlos, centrando la atención y recursos en estos. Los riesgos evaluados como bajos se consideran aceptables por parte de la organización, teniendo en cuenta la situación y contexto actual de nuestra empresa y los recursos disponibles.

Las acciones sobre los riesgos objetivo de tratamiento incluyen acciones como,

- Implementación de nuevos controles
- Revisión y mejora de la efectividad de los controles existentes
- Eliminación del riesgo mediante la decisión de la modificación de la naturaleza de la actividad/proceso que origina el riesgo o cesando la misma.

La planificación del tratamiento de los riesgos y su seguimiento se realiza reflejando las acciones/decisiones/controles para prevenir, mitigar o eliminar el riesgo e indicando en cada caso el documento/proceso/procedimiento de control o bien desarrollándose el mismo en el **Plan de Tareas** asociado a cada control.

El Responsable del Sistema mantiene registro y evidencia de todas las actividades relacionadas con el tratamiento de riesgos en el **R-0201 Evaluación de Riesgos por Procesos**

2.9. Identificación, análisis y tratamiento de oportunidades

Las oportunidades se identifican mediante el análisis del contexto, de las necesidades y expectativas de las partes interesadas, los procesos identificados y utilizando la misma metodología de reuniones y participación descrita para los riesgos.

Es responsabilidad del Responsable del Sistema, la conservación del registro y evidencia de esta actividad periódica de identificación de riesgos en los procesos de nuestra organización

En el **R-0202 Evaluación de oportunidades**, quedarán identificadas las mismas y serán objeto de seguimiento y evaluación continua para comprobar su eficacia.

Quedará a criterio de Dirección abordar una u otra en función de los intereses generales y desarrollo estratégico de **CLÍNICA BEIMAN** y se establecerán para cada una de ellas los recursos necesarios para su consecución. Algunas de ellas serán propuestas como objetivos anuales dentro de nuestro Sistema de Gestión según el contexto actual de la empresa y otras serán incorporadas de manera escalonada según disponibilidad.

3. Apreciación de riesgos por activos

Adicionalmente a este análisis asociado al contexto, se realizará un análisis de los riesgos asociados a los activos de información y a las pérdidas de disponibilidad, integridad y confidencialidad, y que se apoyará en la **IT-0202 Apreciación de Riesgos por Activos**. Este análisis tendrá como base y punto de entrada la identificación de activos.

3.1. Identificación de activos

Como primer paso en este análisis de riesgos, se identificarán todos aquellos activos de información que son empleados para el tratamiento de la información en **CLÍNICA BEIMAN**, considerando, al menos las siguientes categorías de activos de información:

- Hardware (Puestos de usuario, servidores, dispositivos de red, soportes externos, etc.)
- Software (Aplicaciones ofimáticas, KAIROS24H, Intranet, etc.)
- Datos (BBDD, Documentos informáticos de prestación de servicios, Documentación en papel de RRHH, etc.)
- Servicios (Comunicaciones, correo electrónico, alojamiento externo, etc.)
- Personal (Personal interno, colaboradores, etc.)
- Instalaciones (centros, CPD, archivo, etc.)

Para su consideración en el análisis de riesgos, se atenderá al uso de activos “conceptuales”, de modo que pueda realizarse un análisis de riesgos asumible, manejable y efectivo. Esto implica, por ejemplo, que los diferentes puestos de usuario (equipos PC) de los trabajadores de la organización, se introducirán en la matriz de riesgos como un único activo “Puestos de usuario”, entendiendo que todos ellos están sujetos a riesgos similares, y la materialización de los riesgos en cada uno de ellos supondría un impacto similar en la organización.

3.2. Valoración de activos

Una vez identificados, los activos deben ser valorados en términos de Confidencialidad, Integridad y Disponibilidad, dando cumplimiento a los requisitos de la norma de referencia, lo cual determinará la importancia de dichos activos en la organización y, en consecuencia, el impacto que supondría la materialización de un riesgo determinado sobre el activo en particular.

La valoración de los activos se realizará según lo definido en la **IT-0202 Apreciación de Riesgos por Activos.**

3.3. Definición de criterios de aceptación/tolerancia a los riegos

En **CLÍNICA BEIMAN** buscamos reducir todos los riesgos en la medida de lo posible y sometemos a tratamiento todas aquellas conductas, operaciones y/o actividades que obtengan una evaluación de riesgo actual SUPERIOR A BAJO.

3.4. Identificación de riesgos o amenazas

Para la identificación de los riesgos (o amenazas) asociados a nuestros activos de información, tomaremos como referencia las incluidas en el listado de amenazas 'Ejemplo de Amenazas' que se incluye en el **R-0203 Matriz de Riesgos por Activos**, en el que se describen las posibles amenazas que se pueden materializar sobre los diferentes activos de información.

Las diferentes amenazas deben de tener una probabilidad de ocurrencia determinada, que tiene impacto en el valor del riesgo de cada uno de los activos. Para asignar una valoración a la probabilidad de ocurrencia de cada una de las amenazas se seguirá la sistemática y escala definidas en la **IT-0202 Apreciación de Riesgos por Activos**.

3.5. Identificación de vulnerabilidades

El nivel de vulnerabilidad define el grado de protección de los activos de información frente a las diferentes amenazas consideradas. Para determinar el nivel de vulnerabilidad de los activos frente a las amenazas se seguirá lo definido en la **IT-0202 Apreciación de Riesgos por Activos**.

3.6. Cálculo de riesgo actual

En primer lugar, se debe calcular el nivel de riesgo actual, que es aquel que tienen los activos en el momento actual en el que se realiza el análisis de riesgos. Para su cálculo se identificará para cada uno de los activos identificados y valorados, la probabilidad de ocurrencia de cada una de las amenazas considerando el estado actual (sin considerar la aplicación de medidas que se definirán en el Plan de Acción o Plan de Tratamiento de Riesgos), y la valoración de la vulnerabilidad actual (sin considerar la aplicación de medidas) de los activos frente a cada una de las amenazas.

El cálculo de la probabilidad de las amenazas y las vulnerabilidades se podrá realizar según lo definido en **IT-0202 Apreciación de Riesgos por Activos.**

3.7. Tratamiento de riesgos

En **CLÍNICA BEIMAN** hemos determinado actuar, al menos, sobre todos aquellos riesgos cuya evaluación de riesgo actual haya arrojado un nivel POR ENCIMA DE BAJO. Para tales riesgos se definen planes de acción con el objetivo de mitigarlos, centrando la atención y recursos en estos. Los riesgos evaluados como bajos se consideran aceptables por parte de la organización, teniendo en cuenta la situación y contexto actual de **CLÍNICA BEIMAN** y los recursos disponibles.

Las acciones sobre los riesgos objetivo de tratamiento incluyen acciones como,

- Implementación de nuevos controles
- Revisión y mejora de la efectividad de los controles existentes

- Eliminación del riesgo mediante la decisión de la modificación de la naturaleza de la actividad/proceso que origina el riesgo o cesando la misma.

La planificación del tratamiento de los riesgos y su seguimiento se realiza, reflejando las acciones/decisiones/controles para prevenir, mitigar o eliminar el riesgo e indicando en cada caso el documento/proceso/procedimiento de control o bien desarrollándose el mismo en el **Plan de Tareas** asociado a cada activo

3.8. Cálculo de riesgo residual

Una vez analizado y evaluado el riesgo actual, completamos la evaluación del riesgo residual o riesgo final. Todo ello según lo descrito en la instrucción técnica de referencia. (**IT-0202 Apreciación de Riesgos por Activos**).

El riesgo residual nos permitirá conocer el nivel de riesgo que tendrán los activos de información una vez se apliquen las medidas de seguridad previstas en el Plan de Acción, y es el nivel de Riesgo que la organización debe aceptar, considerando su situación actual y los recursos disponibles.

En **CLÍNICA BEIMAN** se aceptarán, por los controles y acciones previamente establecidos, aquellos riesgos de carácter residual cuyo valor sea **MEDIO**.

3.9. Plan de tratamiento de riesgo

Las acciones que se identifiquen en el Plan de Acción de los diferentes sistemas de información se trasladarán al registro **R-0204 Plan de Tratamiento de Riesgo**, donde se identificará, con más detalle, las acciones que se realizarán, con indicación de plazos, responsables, recursos necesarios, etc.

3.10. Declaración de aplicabilidad

La **Declaración de Aplicabilidad** (**RSI-0002**) es un documento que debe acompañar al proceso de análisis de riesgos, como salida de este. En la declaración de aplicabilidad se identificará el estado de aplicación de los diferentes controles recogidos en la norma ISO 27001 indicando aquellos No Aplicados en la organización, aquellos actualmente implementados en la organización, y aquellos que se pretende implementar o mejorar según lo definido en el Plan de Tratamiento de Riesgos.

4. Aprobación de resultados

Para una aprobación formal de los resultados de los análisis de riesgos por parte de la dirección de **CLÍNICA BEIMAN** se realizará el correspondiente **informe revisión por dirección**.

5. Seguimiento y medición

Para la evaluación de la eficacia y el seguimiento de la correcta aplicación de este proceso y las posibles incidencias que puedan encontrarse, se atiende a lo establecido en el documento **P-08 Seguimiento y Medición**.

Para el análisis de la eficacia y/o pruebas de los controles establecidos en el **Plan de Control de Riesgos** se seguirán los criterios definidos en la **IT-0201 Metodología de Apreciación de Riesgos por Procesos.**

6. Revisión y actualización

Las actividades descritas en el presente proceso se realizan y revisan con una periodicidad **mínima ANUAL** o bien en caso de cambios relevantes en el contexto de nuestra organización, o en los activos utilizados para el tratamiento de la información quedando reflejado el resultado en esta actividad en los registros correspondientes haciendo referencia en el apartado correspondiente de "fecha de actualización".

Adicionalmente, durante la **Revisión del Sistema por la Dirección**, se revisan los resultados del seguimiento permanente de este proceso.

7. Seguimiento de planes

Corresponde al Responsable del Sistema de **CLÍNICA BEIMAN**, apoyado por el/los Responsable/s de Proceso/s, llevar a cabo el seguimiento de la adecuación de los Planes de Acción y Tratamiento de riesgos implementados a la realidad de la situación. Las evidencias de dicho seguimiento quedan plasmadas en el apartado de "Seguimiento" dentro de los propios planes de acción.

Adicionalmente, el Responsable del Sistema, durante la Revisión del Sistema por la Dirección, revisa el resultado del seguimiento permanente de estos planes de acción.

8. Formatos y anexos

Documento	Tiempo de archivo de los registros que genera	Responsable
IT-0201 Apreciación de Riesgos por Procesos	3 años	Responsable del Sistema
IT-0202 Apreciación de Riesgos por Activos	3 años	Responsable del Sistema
R-0201 Evaluación de Riesgos por Procesos	3 años	Responsable del Sistema
R-0202 Evaluación de oportunidades	3 años	Responsable del Sistema
R-0203 Matriz de Riesgos por Activos	3 años	Responsable del Sistema

R-0204 Plan de Tratamiento de Riesgo	3 años	Responsable del Sistema

Registro de las modificaciones		
Revisión	**Fecha**	**Naturaleza de la revisión**
00	10/08/2022	Edición inicial