mtech group

Plan de continuidad y contingencias

Versión 3 – Diciembre de 2022

Calle de los albañiles, 3. 28320 Pinto, Madrid, España
+34 917 988 489
mtech@mtechgroup.es
www.mtechgroup.es

ÍNDICE

1. Introducción

La gestión y control de riesgos es un pilar clave en cualquier compañía para asegurar que ésta sea sólida, segura y sostenible, además de estar alineada con los intereses de sus empleados, clientes y de la sociedad, en general.

El objetivo del Plan de continuidad y contingencias del Grupo Mtech es:

- Identificar, evaluar y analizar todos los riesgos a los que está expuesto el Grupo de manera que se puedan aplicar medidas adecuadas para reducir su probabilidad y/o severidad;
- Gestionar de forma adecuada los riesgos que puedan surgir, estableciendo las pautas a aplicar en los diferentes niveles del Grupo para tratar y comunicar un riesgo en caso de existencia;
- Garantizar buenas prácticas de gobernanza;
- Asegurar la continuidad del negocio.

Dicho Plan ha sido aprobado por el Comité de Dirección del Grupo. Anualmente éste será revisado de nuevo por los miembros del Comité, observando, actualizando y aplicando las nuevas exigencias en términos de cultura de riesgos.

2. Modelo de gobierno para la Gestión y control de riesgos

El Grupo Mtech ha considerado un modelo de tres líneas de Gestión y control de riesgos.

En una primera línea se encuentra el seguimiento y control diario de los riesgos que realizan cada uno de los **departamentos y unidades de negocio** del Grupo con el apoyo de políticas y procedimientos específicos a su actividad.

Adicionalmente, en una segunda línea, se sitúa el **Comité de gestión de riesgos**, de carácter informativo y ejecutivo, cuyos miembros son los del Comité de Dirección del Grupo Mtech.

Su cometido consiste:

- Asegurar una comunicación interna/ externa adecuada para la gestión de cualquier evento que pueda comprometer la seguridad de las personas, la continuidad del servicio, el medio ambiente, la protección de activos, la imagen y reputación del Grupo y gestión;
- Garantizar la claridad, velocidad y eficiencia de la toma de decisiones;
- Minimizar los impactos para garantizar una rápida restauración de las condiciones normales de operación;
- Liderar la implantación de los mecanismos de gestión, control y mitigación de riesgos, así como de dar soporte a todos los departamentos que conforman la primera línea de gestión y monitorización de riesgos.

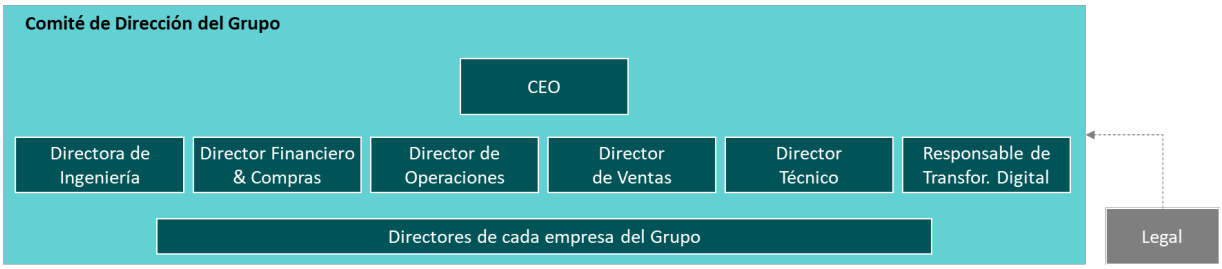

Ilustración 1. Composición del Comité de Gestión de Riesgos del Grupo

Finalmente, como tercera línea, existe el departamento de Calidad y Medio ambiente de Mtech, encargado de llevar a cabo **auditorías internas** para velar por el cumplimento de las políticas definidas en términos de gestión de riesgos y prestar asesoramiento independiente y objetivo al Comité de gestión de riesgos.

Cada una de estas tres "líneas" tiene la obligación de informar y mantener actualizada a la línea superior, siendo el Comité de gestión de riesgos el máximo responsable.

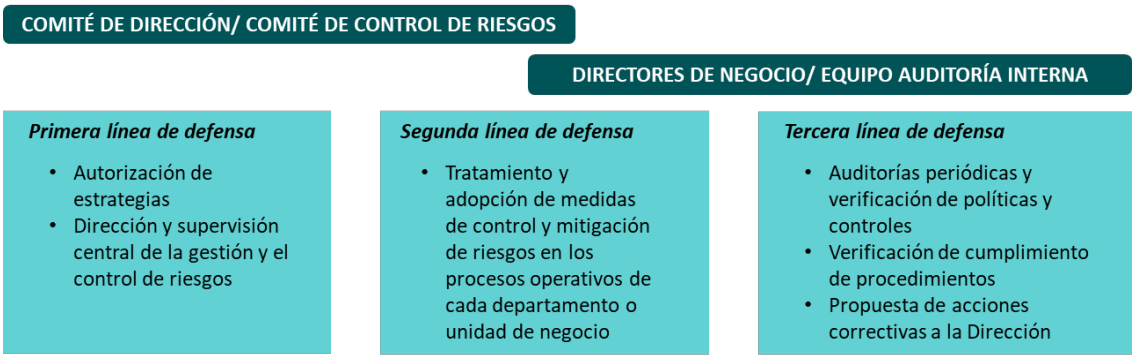

Ilustración 2. Sistema de Gestión de Riesgos del Grupo Mtech

3. Principales riesgos identificados y mecanismos de gestión

La identificación y el análisis de los riesgos Ambientales, Sociales y de Gobierno que afectan al negocio del Grupo se ha realizado por el equipo de Auditoría Interna, involucrando de forma directa a todas las departamentos y unidades responsables, creando conciencia y cultura de la relevancia de este tema para el Grupo. Como resultado a este análisis, el Grupo ha obtenido como un **Mapa de riesgos**. Para cada uno de los principales riesgos, Mtech ha definido además medidas específicas de gestión.

Tabla 1. Principales riesgos y mecanismos de gestión del Grupo Mtech

Riesgo identificado	Mecanismos de gestión para su mitigación
RIESGOS NATURALES	
Potenciales problemas derivados de catástrofes o desastres asociados a peligros naturales	- Conformación del grupo *Brigada de emergencias* para llevar a cabo: diagnóstico, planeación, ejecución y evaluación para realizar correctivos. En caso de ser necesario, este grupo es el responsable de solicitar los apoyos requeridos, a los distintos organismos, en función de los niveles de emergencia o gravedad del evento. Para ello, este grupo ha recibido una formación específica y dispone de todos los medios humanos y mecánicos necesarios para mitigar el impacto. - Realización periódica de simulacros corporativos: simulacros de evacuación, simulacros de extinción de incendios, simulacros de primeros auxilios y simulacros generales. - Contratación de seguros para hacer frente a catástrofes o desastres ocasionados por peligros naturales. - Transferencia de las operaciones a filiales del Grupo ubicadas en otra localización (por ejemplo de Madrid a Vizcaya o de Vizcaya a Madrid).
RIESGOS OPERATIVOS	
Incertidumbre asociada a la demanda de servicios y productos en un entorno cambiante	- Dimensionamiento de recursos para hacer frente a todos los proyectos. - Seguimiento comercial a principales clientes. - Prospección de nuevos clientes. - Seguimiento a oportunidades por cambios y asignación de nuevos presupuestos.
Fallo del sistema de suministro y/o interrupciones	- Diversificación de proveedores, en compañías y geográficamente.
Ciberataque	Véase el punto 5 de este documento para mayor detalle
RIESGOS ESTRATÉGICOS	
Dificultades de adaptación a los distintos entornos regulatorios	- Asesoramiento legal y fiscal. - Seguimiento de actualizaciones de normativas. - Transferencia al cliente con regulación de cláusulas de cambio de ley y variaciones.
Inestabilidades políticas y sociales	- Asesoramiento legal y fiscal. - Seguimiento de actualizaciones de normativas. - Transferencia al cliente con regulación de cláusulas de cambio de ley y variaciones.
Creciente competitividad de la industria	- Inversión en I+D+i. - Nuevos productos. - Estudio de sinergias y nuevas líneas de negocio. - Sistemas de mejora continua. - Acuerdos con actores claves dentro de la Industria.
Reducción de los precios de venta y/o aumento de los precios de compra	- Optimización de precios de proveedores. - Optimización del diseño mediante inversión en I+D+i. - Establecimiento de acuerdos marco con proveedores. - Seguimiento a la fluctuación del precio de las materias primas.
Seguridad de la información. Propiedad intelectual e industrial, y no divulgación externa	- Designación de un responsable de seguridad. - Definición de una política de ciberseguridad y aplicación. - Concienciación y formación en ciberseguridad. - Realización de una auditoría de seguridad. - Firma formulario de compliance.
RIESGOS NORMATIVOS	
Adaptación a potenciales cambios normativos	- Asesoramiento legal y fiscal local. - Transferencia al cliente con regulación de cláusulas de cambio de ley y variaciones.
Potenciales incumplimientos normativos a nivel operativo	- Asesoramiento legal y fiscal local. - Seguimiento de actualizaciones de normativas de diseño locales. - Transferencia al cliente con regulación de cláusulas de cambio de ley y variaciones. - Requerimiento de especificaciones de proyecto específicas a los clientes.

Tabla 2. Principales riesgos y mecanismos de gestión del Grupo Mtech

Riesgo identificado	Mecanismos de gestión para su mitigación
RIESGOS FINANCIEROS	
Mercado (tipo de cambio/tipo de interés) o crisis económica	- Contratación de coberturas. - Seguimiento a las fluctuaciones de los tipos. - Acuerdos con proveedores en la misma moneda que el contrato principal. - Acuerdos marco con entidades financiadoras.
Liquidez	- Acuerdos marco con entidades financiadoras. - Revisión de nuevas fórmulas de financiación. - Acuerdos marco con proveedores/clientes. - Revisión del flujo de caja de proyectos previo a la firma del contrato, conforme a las condiciones de pago del cliente y a proveedores. - Análisis del riesgo máximo de impago. - Seguimiento al flujo de caja de proyectos en ejecución.
Crédito a clientes	- Revisión del flujo de caja de proyectos previo a la firma del contrato, conforme a las condiciones de pago del cliente y a proveedores. - Análisis del riesgo máximo de impago. - Seguimiento al flujo de caja de proyectos en ejecución.
Obtención garantías necesarias para poder contratar/ejecutar proyectos	- Acuerdos marco con entidades financiadoras/aseguradoras. - Seguimiento activo de la situación avales emitidos y de la posición global - Negociación con clientes. - Fortalecimiento balance.
RIESGOS SOCIALES	
Pandemias o crisis sanitarias	- Cultura de seguridad y salud laboral. - Definición, aplicación y seguimiento de políticas en términos de seguridad y salud laboral. - Integración de la seguridad en los procesos operativos. - Formación al personal propio y/o subcontratado.
Accidentes en el personal propio y/o subcontratado	- Cultura de seguridad y salud laboral. - Definición, aplicación y seguimiento de políticas en términos de seguridad y salud laboral. - Integración de la seguridad en los procesos operativos. - Formación al personal propio y/o subcontratado.
Atracción y retención de trabajadores	- Definición y comunicación de políticas de diversidad. - Gestión y promoción del talento. - Conciliación de la vida laboral con la vida personal. - Promoción de la educación y crecimiento de las personas mediante formación.
RIESGOS DE GOBERNANZA	
Conductas ilícitas, actividad de lobby, entre otras, por parte de personal propio o contratado, o de prácticas anticompetitivas	- Definición y publicación de un Código ético y de una política de anticorrupción. - Creación de un canal de comunicación para abordar estos temas.

4. Gestión de la sostenibilidad

4.1. Contribuciones específicas a Objetivos de Desarrollo Sostenible

Uno de los objetivos del **Comité de gestión de riesgos** es asegurar la sostenibilidad y continuidad del negocio.

Mtech Group se ha comprometido a hacer contribuciones específicas a seis de los **3 Objetivos de Desarrollo Sostenible**: Igualdad de género (ODS 5), Trabajo decente y crecimiento económico (ODS 8), Ciudades y comunidades sostenibles (ODS 11).

Este compromiso ha sido incorporado al plan estratégico de Mtech Group. Su no cumplimiento representa un riesgo para la continuidad de la Compañía.

Ilustración 3. Integración de los distintos Objetivos de Desarrollo Sostenible en la taxonomía de riesgos definida para el Grupo Mtech

4.2. Desempeño Ambiental

El Grupo Mtech ha publicado un **Comunicado de Desempeño Ambiental** en la página web corporativa en donde se hace referencia al compromiso de la compañía con la protección y conservación del Medio Ambiente, a través de un Sistema de Gestión según dicta la norma UNE-EN ISO 14001:2015.

4.3. Responsabilidad Social Corporativa

Mtech Group entiende la **Responsabilidad Social Corporativa** como la responsabilidad que le corresponde al Grupo por el impacto de su actividad en la Sociedad. Para cumplir con esta responsabilidad, Mtech Group integra las preocupaciones sociales, medioambientales, éticas, sobre derechos humanos y de los grupos de interés o Stakeholders en su negocio diario y en las relaciones con ellos en su **Política de Responsabilidad Social Corporativa**, publicada en la página web corporativa.

5. Ciberseguridad

El área de Transformación digital del Grupo Mtech es la responsable de la **ciberseguridad** a nivel corporativo.

Un ciberataque es un ataque organizado contra el sistema informático de una entidad o empresa con el objetivo de bloquearlo, dañarlo u obtener información.

Ante un ciberataque, cualquier empleado de Mtech Group deberá avisar al líder de Seguridad Informática o responsable del área de Transformación digital de la organización, quién establecerá las directrices para la ejecución de procesos.

Cuando la amenaza sea detectada, el líder de Seguridad Informática informará a la primera línea y se establecerá el estado de emergencia y se activarán los protocolos de seguridad.

A continuación, se especifican las acciones a llevar a cabo:

- **Líder de la Seguridad Informática**
  - Detectar ataque en el sistema.
  - Establecer el impacto de la amenaza.
  - Informar a la primera línea de un evento crítico.
  - Coordinar con la segunda y tercera línea la aplicación del Plan de contingencia.
- **Centro de soporte IT**
  - Informar sobre novedades durante y después del ataque al líder de Seguridad Informática y al resto de empleados.
  - Dar soporte a usuarios internos y detectar si alguno se encuentra comprometido con algún código malicioso. De encontrarse infectado, proceder a aislarlo e indicar al usuario de apagar su estación para evitar la propagación de la amenaza.
  - Bloqueo del perímetro interno y externo.
  - Coordinar con proveedores de enlaces, los cambios de ruta del tráfico interno y externo hacia el Centro de Datos Virtual (CDV).
  - Actualizar reglas del firewall en el CDV y configuraciones de switch y Router (en caso de ser necesario).
  - Tener disponible los últimos respaldos de las copias de seguridad (última versión estable) de la base de datos, de las aplicaciones y del sistema en general.
  - Realizar pruebas de compatibilidad y funcionamiento en el CDV.
  - Replicar configuraciones en las instalaciones del CDV para continuar operaciones desde la contingencia.
  - Monitorizar el sistema y verificar funcionamiento de los servicios.
  - Aislar los servidores de la red interna.
  - Verificar si servidor está comprometido y apagarlo en caso afirmativo.
  - Verificar y aplicar respaldos en servidores del CDV con el apoyo del Centro de computación.
  - Verificar actualizaciones en servidores del CDV.
  - Verificar procesos en servidores del CDV.
  - Actualizar almacenamiento de datos en CDV (si necesario).

- **Control de calidad**
    - Verificar los cambios aplicados por el equipo de soporte IT, y certificar su óptimo funcionamiento.
    - Certificar las pruebas de funcionamiento de las aplicaciones del CDV.
- **Marketing**
    - Si aplica, a través de las redes sociales de la empresa, informar públicamente del estado de emergencia y proceso de subsanación para su solución inmediata
    - Éste es la única área autorizada por la primera línea y el líder de Seguridad Informática para emitir comentarios sobre el estado de la empresa sin menoscabar la confianza del público en el tratamiento de sus valores.

A continuación, se describe el procedimiento de respuesta a seguir en caso de un ciberataque.

5.1.1. Fase de alerta

La fase de alerta puede ser informada por cualquier usuario interno, ya sea porque su equipo está con un comportamiento anormal o algún detalle que haya notado al realizar sus labores diarias.

El líder de Seguridad Informática, junto con la ayuda del área de Soporte IT, deberá evaluar el evento.

Se revisará el sistema para detectar posibles infecciones o intrusiones.

De esta fase dependerá el impacto que el ciberataque o amenaza tenga sobre el negocio y también la ejecución del plan de contingencia.

5.1.2. Fase de transición

La fase de transición abarcará el paso de las operaciones desde el centro de datos principal hacia el centro de datos virtual (contingencia) para poner reanudar en el menor tiempo posible las operaciones.

Se declarará así el estado de emergencia en la empresa y los equipos técnico y no técnicos implicados ejecutarán las tareas asignadas, siempre bajo la coordinación del líder de Seguridad Informática y de la primera línea.

5.1.3. Fase de recuperación

En esta fase se incluyen todas las acciones para la puesta en producción del Centro de Datos Virtual con la carga de información de las bases de datos, sistemas operativos y aplicaciones internas y externas. Así mismo, se incluyen aquí las pruebas de funcionamiento de todo el sistema por parte de los diferentes equipos tecnológicos.

5.1.4. Vuelta a la normalidad

Una vez ocurrido el evento, habiendo recuperado el sistema a través del Centro de Datos Virtual, es necesario realizar algunos pasos para regresar a operaciones normales una vez superado el incidente.

- **Planificar**

Se deberá planificar la vuelta a operaciones normales una vez que la amenaza se encuentre controlada y los sistemas hayan sido restaurados (si fuera necesario), garantizando su funcionamiento.

- **Evaluar daños**

Se detallarán los daños que se han producidos por el ciberataque, vulnerabilidades en las comunicaciones, especialmente los firewalls, posibles daños en la base de datos (si hubiere), y en general se realizará una evaluación al sistema para determinar si se han sufrido daños que comprometan su integridad y necesiten reparación física o lógica para regresar a operaciones en el Centro de Datos Principal.

- **Priorizar y ejecutar actividades**

Los equipos del área de tecnología realizarán las actividades para restaurar lo que tenga algún fallo lógico o físico.

- **Comunicar**

Durante la emergencia, el líder de la Seguridad Informática, apoyándose en los equipos técnicos y no técnicos implicados, responderá e informará de avances de su trabajo de restauración a la primera línea y liderará la comunicación al resto de usuarios impactados.

Sólo podrá emitir comunicados externos, el área de Marketing, siguiendo las indicaciones del líder de la Seguridad Informática y de la primera línea.

- **Retroalimentar**

Dependiendo de la seriedad del ciberataque, la vuelta a la normalidad puede tomar unas horas hasta varios días. El objetivo es que el servicio hacia los clientes no se detenga y el trabajo de los usuarios internos de la empresa no se vean afectados en mayor medida.

Con el objetivo de obtener mejores resultados en futuras ocasiones similares, el equipo técnico deberá analizar, recabar e informar al líder de la Seguridad Informática de los acontecimientos para ajustar el procedimiento actual, si necesario.