Política de gestión de riesgos

[Soggetto]

1 Control de versiones de documentos

	Última modificación	**Última modificación**	**Cambios en el documento**
0.1	[FECHA]		Documento creado por primera vez

2 Índice

3 Política de gestión de riesgos

3.1 Propósito

El objetivo de esta política es definir la política de gestión de riesgos de la empresa en materia de seguridad de la información

3.2 Destinatarios

Todos los empleados y usuarios de terceros.

Riesgo y gestión del riesgo aplicados a la seguridad de la información y a la confidencialidad, integridad y disponibilidad de la información poseída, procesada, almacenada y transmitida por la organización.

3.3 Principio

La gestión de la seguridad de la información de la empresa se basa en una gestión adecuada y apropiada de los riesgos.

3.4 ¿Qué es la gestión de riesgos?

El riesgo puede definirse como la amenaza o posibilidad de que una acción o acontecimiento afecte negativa o positivamente a la capacidad de una organización para alcanzar sus objetivos.

La gestión de riesgos puede definirse como la aplicación sistemática de principios y enfoques y un proceso mediante el cual una empresa identifica y evalúa los riesgos asociados a sus actividades y, a continuación, planifica y pone en práctica respuestas al riesgo.

3.5 Apetito de riesgo

En general, la empresa tiene una propensión al riesgo moderada, lo que significa que los riesgos se mitigan de forma rentable y proporcional al riesgo y que es aceptable una cierta aceptación del riesgo en función de las necesidades de la empresa.

3.5.1 Baja propensión al riesgo

La empresa tiene una baja propensión al riesgo, lo que significa que no se aceptarán riesgos y que dispondrá de recursos asignados para mitigarlos de forma proporcionada y rentable:

- Acceso, uso o divulgación no autorizados de información personal identificable o datos sensibles.

- Incumplimiento de leyes, reglamentos, políticas o procedimientos relativos a la tecnología.
- Falta de resistencia frente a las amenazas de ciberseguridad.

3.6 Identificación y evaluación de riesgos

Las evaluaciones de riesgos se llevan a cabo a intervalos regulares o al menos cada 12 meses y cuando se han producido o pueden producirse cambios significativos.

Los riesgos se identifican y evalúan al menos para

- El tratamiento, almacenamiento o transmisión de información confidencial, personal o del titular de la tarjeta
- Terceros proveedores que procesan, almacenan o transmiten información confidencial, personal o del titular de la tarjeta
- Nuevos sistemas
- Cambios significativos

3.7 Registro de riesgos

Todos los riesgos se registran en el registro de riesgos de la empresa.

3.8 Señalización de riesgos

El registro de riesgos se revisa durante la reunión del equipo de revisión.

Los riesgos se comunican al Equipo de Revisión

Los riesgos significativos, identificados como riesgos que requieren la atención de la alta dirección o riesgos con una puntuación superior a 20 o riesgos clasificados como graves, se comunican a la alta dirección y forman parte de los informes corporativos de gestión de riesgos de la empresa.

3.9 Revisión de riesgos

Los riesgos se revisan y supervisan periódicamente durante la reunión del Equipo de Revisión para garantizar:

- Avance de la acción contra el riesgo
- Eficacia de la acción contra el riesgo
- Gestión del riesgo residual

3.10 Tratamiento del riesgo

Se asigna un gestor de riesgos a todos los riesgos

3.10.1 Aceptación del riesgo

La decisión de aceptar riesgos corresponde al jefe del departamento correspondiente y/o a la alta dirección.

El criterio para aceptar el riesgo se basa en estos criterios

- El riesgo se clasifica como bajo y no es conveniente tratarlo.
- Existe una oportunidad comercial o empresarial que justifica la amenaza y el impacto.
- No hay tratamiento de riesgo
- El impacto de que se produzca el riesgo es aceptable para la empresa

3.10.2 Reducción de riesgos

Cuando haya que mitigar un riesgo

- El responsable del departamento correspondiente y/o el Equipo de Revisión y/o la Alta Dirección aprueban un plan de acción.
- Se asigna la responsabilidad de la aplicación y gestión del plan.
- Los riesgos se comunican y revisan durante la reunión del equipo de revisión de la gestión y se anotan en el registro de riesgos.

3.11 Evaluación de riesgos

La evaluación del impacto del riesgo se considera en función de:

- Cumplimiento y legislación
- Reputación
- Clientes
- Metas y objetivos de la empresa
- Resultados financieros

Cumplimiento de las normas

3.12 Medición del cumplimiento

El equipo de gestión de la seguridad de la información supervisará el cumplimiento de esta política a través de diversos métodos, incluidos, entre otros, los informes de las herramientas de la empresa, las auditorías internas y externas y la información al responsable de la política de seguridad de la información.

3.13 Excepciones

Cualquier excepción a la política debe ser aprobada y registrada previamente por el responsable de seguridad de la información y comunicada al equipo de revisión de la gestión.

3.14 Incumplimiento

El empleado que infrinja esta política podrá ser objeto de medidas disciplinarias de hasta .

3.15 Mejora continua

La política se actualiza y revisa en el marco del proceso de mejora continua.