Política de Seguridad y riesgos

Prisma - Departamento

Documento de uso interno

Índice

VERSIÓN 3
INTRODUCCIÓN Y MARCO NORMATIVO 4
Normas de referencia 5
Anexo - Gestión de crisis 6
Roles y responsabilidad del Comité de Crisis 6
Procedimiento general de gestión de crisis 7
Detección de la crisis 7
Activación del Comité de Crisis 8
Evaluación y categorización de la crisis 9
Comunicación 10
Mitigación 10
Resolución 10
Lecciones aprendidas 10
Plan de formación y seguimiento 11

VERSIÓN

Versión	Fecha	Autor	Revisor	Aprobada	Comentarios
1.0	15/07/2025	Audea	Rubén Utrilla	comité	Versión Inicial

INTRODUCCIÓN Y MARCO NORMATIVO

La Dirección de PRISMA quiere dar a conocer, a través de este documento, a sus trabajadores, clientes, proveedores y otras partes interesadas su convencimiento de que la Seguridad de la Información es un factor clave para el correcto desarrollo de la organización.

Prismapay considera que tanto la Gestión de la Seguridad de la Información, junto con la dotación de formación y recursos necesarios para el desarrollo de la actividad propia de esta organización, esto es, la prestación de servicios de pagos integrados (Integrated Payments), el procesamiento seguro de transacciones financieras, el desarrollo e integración de pasarelas de pago (APIs), y la gestión de plataformas de cobro, así como la implantación o utilización de Infraestructura, plataforma y Software que soporte dichos servicios, son los principales pilares en los que se fundamenta el trabajo y esfuerzo diario.

Para ello, el Sistema de Gestión de Seguridad de la Información tiene como objetivos:

1. Gestión de la Seguridad de la Información, conforme a las Normas:
    a. ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management
    b. ISO/IEC 27001 Information technology – Security techniques – Information Security Management Systems – Requeriments
    c. ISO/IEC 22301 Societal security — Business continuity management systems — Requirements
    d. Digital Operational Resilience Act (DORA) es el Reglamento (UE) 2022/2554.
2. Asignación eficaz de funciones y responsabilidades.
3. Servicios de una calidad y seguridad de la información que satisfagan y superen las necesidades de nuestros clientes.
4. Prevención de posibles defectos y posibles incidentes de seguridad de la información antes de que ocurran, trabajando orientados hacia la “mejora continua” y la comunicación.
5. Gestión y control eficaz del proceso productivo mediante personal cualificado y especializado en la actividad de la empresa en la búsqueda de la Mejora continua de los procesos, procedimientos, productos entregados y servicios prestados al cliente, alcanzando a lo largo del tiempo una mayor madurez en su gestión y ejecución.
6. Formación necesaria del personal conforme a los cambios técnicos e innovaciones tecnológicas a la que la actividad de la organización se viera sometida, para una ejecución del trabajo con los

niveles de calidad y seguridad de la información exigible.

7. Evolución continua del Sistema de Gestión de Seguridad de la Información, con el fin de adecuarnos a las exigencias de nuestros clientes, a través de:
    a. Revisiones continuas del Sistema de Seguridad de la Información.
    b. Establecimiento de indicadores de seguridad que nos permitan conocer el grado de eficacia y seguridad de nuestros procesos productivos.
    c. Fomento de la formación del personal de la organización en los aspectos débiles que se detecten a lo largo del ejercicio.
    d. Búsqueda y desarrollo de nuevos documentos que describan con mayor claridad las actividades a realizar dentro de la organización (procedimientos, generales y específicos, etc.) y a su posterior implantación.
    e. Realización de auditorías de seguridad periódicas para conocer el grado de cumplimiento de la política de seguridad.
    f. Establecer el nivel de seguridad basándose en análisis de riesgos.
8. Concienciación y motivación del personal de PRISMA sobre la importancia de la implantación y desarrollo de un Sistema de Gestión de Seguridad de la Información.
9. Asegurar el cumplimiento de la legislación, reglamentación y normativas aplicables, así como todos aquellos requisitos que la organización considere oportunos llevar a cabo para mantener un sistema de gestión de seguridad de la información formal, que le permita conseguir una mejora continua de su actuación.
10. Analizar los riesgos a los que está expuesta la Organización, y gestionarlos de la mejor forma posible para alcanzar el nivel de Riesgo aceptado por la máxima Dirección, y analizar las oportunidades a través el análisis de contexto.

Normas de referencia

Para el desarrollo del presente procedimiento, nos hemos apoyado en los estándares de seguridad reconocidos internacionalmente y en la normativa interna que recogemos en la siguiente tabla:

- ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management
- ISO/IEC 27001 Information technology – Security techniques – Information Security Management Systems – Requeriments
- ISO/IEC 22301 Societal security — Business continuity management systems — Requirements
- Digital Operational Resilience Act (DORA) es el Reglamento (UE) 2022/2554.

Anexo - Gestión de crisis

PROCEDIMIENTO GESTIÓN DE CRISIS

Con el objetivo de garantizar una respuesta integral y coordinada ante una situación de crisis, esta debe ser gestionada desde dos enfoques complementarios:

- Enfoque operativo o técnico: centrado en la remediación y/o mitigación del incidente, mediante la actuación conjunta del equipo de respuesta ante incidentes y del equipo técnico de la organización.
- Enfoque de coordinación organizativa: liderado por el equipo directivo, encargado de gestionar la situación de especial gravedad y de facilitar el proceso de toma de decisiones estratégicas.

Roles y responsabilidad del Comité de Crisis

La decisión de escalar un incidente a la categoría de situación de crisis será responsabilidad del Comité de Crisis. Para ello, resulta fundamental analizar de forma rigurosa el impacto potencial del incidente y sus posibles consecuencias para la organización. El Comité de Crisis actuará como el máximo órgano responsable en la gestión de situaciones de crisis, y deberá estar previamente constituido y definido. Su función principal será agilizar el proceso de toma de decisiones, con el objetivo de resolver y/o mitigar de manera efectiva las incidencias producidas, estableciendo de forma clara las prioridades y definiendo tanto la estrategia como la táctica a seguir. El Comité de Crisis estará compuesto por un grupo reducido de personas con perfiles complementarios, ejecutivos y altamente resolutivos, con capacidad de actuar con eficacia en situaciones de caos, estrés o elevada presión.

El Comité estará formado, como mínimo, por los siguientes miembros:

- Responsable del Comité de Crisis (con máxima capacidad de decisión, en este caso el CEO de la compañía).
- Responsables de operaciones
- Responsable de los Sistemas de Gestión de Seguridad de la Información y de Continuidad de Negocio.
- Responsable Legal.
- Responsable Financiero.

Las funciones específicas de cada uno de los miembros estarán detalladas en los documentos correspondientes a cada área, tales como:

- Política de Seguridad.

- Política de Continuidad de Negocio.
- Procedimiento de Comunicación.

Procedimiento general de gestión de crisis

Definimos el procedimiento de gestión de crisis como aquellos procesos que han sido diseñados para dar respuesta a una situación de crisis en la organización, y cuyas fases pasamos a describir a continuación:

Detección de la crisis

Como ya se ha indicado anteriormente, Prisma considera una crisis como cualquier situación de especial gravedad que requiera una respuesta integral, coordinada y ejecutada a alto nivel, y que pueda comprometer no solo la continuidad del negocio, sino también afectar a los objetivos estratégicos, la reputación corporativa o provocar pérdidas financieras significativas, pudiendo incluso poner en riesgo el futuro de la organización.

Cualquier empleado de Prisma puede ser el primero en detectar un evento con el potencial de desencadenar una situación de crisis, motivo por el cual es fundamental que las decisiones se adopten con la máxima rapidez, siempre con el objetivo de minimizar el impacto para la organización.

Una vez identificado un evento que pudiera evolucionar hacia una crisis organizacional, será necesario proceder a la activación del Comité de Crisis, con el fin de garantizar una respuesta ágil y eficaz desde las primeras fases de la gestión.

Activación del Comité de Crisis

A continuación, se deberá determinar qué elementos de la organización han sido afectados por el incidente que ha generado la crisis.

Esta fase implica recopilar, analizar y comprender las circunstancias, tecnologías, procesos y recursos de la organización que se han visto comprometidos, con el objetivo inicial de mitigar el impacto y contener el incidente.

Una vez evaluado el alcance inicial del incidente, Prisma deberá establecer su nivel de impacto, categorizándolo de la siguiente manera:

- Gravedad baja: incidente menor que puede ser gestionado internamente, sin riesgo para la continuidad del negocio, la reputación o el impacto financiero. En este caso, no será necesaria la activación del Comité de Crisis, aunque sí se deberá remitir un informe del incidente al mismo. Un ejemplo podría ser una incidencia técnica crítica que haya provocado una interrupción breve de un servicio, resuelta sin necesidad de activar planes o procedimientos específicos.
- Gravedad media: incidente de impacto moderado que, en principio, puede resolverse internamente y que no afecta a la operativa general ni implica pérdidas reputacionales o financieras. Al igual que en el caso anterior, no se requiere activar el Comité de Crisis, pero este deberá ser informado.
- Gravedad alta: incidente que compromete significativamente los procesos, la reputación o puede derivar en pérdidas financieras relevantes. Debe involucrarse a todo el Comité de Crisis para su gestión y resolución.
- Gravedad crítica: incidente que pone en riesgo la continuidad del negocio, con consecuencias potencialmente muy graves para Prisma en términos financieros, reputacionales u operativos. Requiere una respuesta ejecutiva de máximo nivel, por lo que la activación inmediata del Comité de Crisis es obligatoria.

La clasificación del nivel de gravedad se determinará según la tipología del evento, conforme al procedimiento de gestión aplicable en cada caso (por ejemplo, incidentes de seguridad de la información, indisponibilidad de sistemas o brechas de seguridad).

En esta fase inicial del procedimiento, para incidentes relacionados con la seguridad o la tecnología, será el equipo de IT —específicamente el área de Ciberseguridad— junto con el CTO, quienes tendrán la responsabilidad de informar al Comité de Crisis sobre los hechos ocurridos, con el fin de valorar la necesidad de su activación.

Asimismo, cualquier miembro del Comité de Crisis que tenga conocimiento de un incidente con potencial de afectar al negocio, deberá ponerlo en conocimiento del resto del Comité, lo que podría conllevar su activación.

Adicionalmente, el Responsable del Comité de Crisis podrá convocarlo en cualquier situación que

considere como un evento potencialmente disruptivo para la organización.

Evaluación y categorización de la crisis

Aunque no hay una forma estándar de predecir todas las crisis, si es posible clasificarlas en categorías, con el objetivo de crear planes con base en lo que podría suceder:

- **Incidentes que afecten a la seguridad de la información**: en aquellos casos en los que el incidente afecte a la seguridad de la información de Prisma, se deberá evaluar junto con el servicio de respuesta ante incidentes externos, y será necesario llevar a cabo un conjunto de actuaciones que deben afrontarse siguiendo las pautas que recogemos en el documento "**PES.16 Gestión de Incidentes de Seguridad de la Información**".

    - **En el caso de que el incidente afecte a la disponibilidad,** y por tanto, es posible que afecte a la continuidad de negocio, será necesario activar el plan de continuidad de negocio. En el documento "**PES 17. Política de Continuidad de Negocio**" se describen los pasos a seguir para activar el plan de continuidad de negocio.

    - Del mismo modo, **en aquellos casos en los que el incidente afecte a la confidencialidad de los datos**, y como consecuencia se pueda producir una brecha de seguridad que afecten a datos personales, deberemos actuar tal y como indicamos en la política de brechas de seguridad "**PES16.02 Política Brechas de Seguridad**"

- **Perdida financiera**: en aquellos casos en los que la situación de crisis tenga como consecuencia una perdida financiera, el Comité de Crisis será el encargado de evaluar su dimensión y deberá buscar mecanismos o acciones que permitan mitigar la perdida, ya que una perdida financiera podría provocar la bancarrota o incluso tomar medidas drásticas como puede ser el despido de empleados o la perdida de carteras por parte de clientes.

- **Desastre natural**: posibilidad de que un desastre natural (huracanes, incendios, descargas eléctricas, inundaciones, …) puedan dar lugar a una parada del negocio. Afectando generalmente a la disponibilidad, este tipo de crisis deben tenerse en cuenta dentro del análisis de riesgos integrado en el sistema de gestión de la continuidad de negocio.

- **Cambios operativos o fallos humanos**: si bien es cierto que un cambio operativo no suele dar lugar a la activación de una crisis en la organización, es posible que se den cambios que puedan afectar en el día del negocio, como podría ser un cambio inesperado en el liderazgo o de personal crítico para el negocio. Frente a esta situación, será el Comité de Crisis el encargado de buscar y aplicar soluciones para mitigar los efectos que el cambio operativo pueda producir. Esta tipología también debe contemplarse dentro de los riesgos de la continuidad de negocio.

- **Daño reputacional o de imagen**: en cualquier ámbito o tipo de organización, existe la posibilidad de que se produzca un daño reputacional, que podría ser originado por múltiples motivos. En estos casos, la organización deberá estar preparada para afrontar este tipo de problemas que pueden dar lugar a activar el plan de crisis en Prisma.

Comunicación

Todas las decisiones y actuaciones relacionadas con el incidente deberán ser tomadas y coordinadas por el Comité de Crisis. En función de la tipología del incidente y su impacto, será necesario mantener informados a nuestros principales grupos de interés, tanto internos como externos, así como a los medios de comunicación en caso de ser necesario. Disponemos de un plan de comunicaciones desarrollado en el documento "**Procedimiento de Comunicación".**

En esta fase previa del análisis de impacto del incidente producido, será necesario evaluar si es necesario contactar con el equipo de respuesta ante incidentes externo (CERT), activar el seguro de ciber riesgo, u otros servicios externos de apoyo que puedan ser necesarios para ayudarnos en la resolución de la crisis.

Mitigación

Una vez activado el Comité de Crisis y determinados qué elementos de la organización han sido afectados por el incidente que ha generado la crisis, es necesario elaborar y comprender las circunstancias, tecnologías, procesos y recursos de la organización que se han visto afectados, con el objetivo, en primer lugar, de mitigar y bloquear el ataque.

En caso de que no sea posible impedir la crisis, el mejor paso a seguir es controlarla o contenerla. Esta etapa recibe el nombre de contención, y tiene como finalidad disminuir los efectos propios que la crisis puede tener en Prisma, siempre con el objetivo de que afecte lo menor posible a la continuidad del negocio.

Cada tipología de crisis tiene una metodología de mitigación diferentes, estas se describen en cada procedimiento especifico, especialmente aquellas crisis relacionadas con continuidad de negocio e incidentes de seguridad cuya gestión se encuentra procedimentada específicamente en los planes de continuidad de negocio y gestión de incidentes de seguridad.

Resolución

Una vez que la situación de crisis ha sido controlada, es imprescindible actuar rápido, siempre con el objetivo de resolver el incidente para volver a la normalidad lo antes posible.

A partir de las estrategias de recuperación escogidas por el Comité de Crisis, se realizará la selección e implantación de las iniciativas necesarias, y se documentará en caso de ser necesario para recuperar la normalidad en la organización, tratando de recuperar en todo momento los entornos afectados.

Lecciones aprendidas

Una vez vuelto a la normalidad y dada la crisis por finalizada, es necesario obtener un aprendizaje de lo sucedido, ya que forma parte de todas aquellas actividades posteriores a la crisis en donde el Comité de

Crisis podrá evaluar si la estrategia y las soluciones aplicadas han sido las mejores, así como de identificar acciones de mejora que puedan reforzar los controles existentes de la organización y puedan mitigar o eliminar el impacto de que se produzca una nueva situación de crisis en el futuro.

Del mismo modo, se deberá revisar el plan de gestión de crisis aplicado con el objetivo de verificar si se han seguido todos los pasos requeridos o si, por el contrario, es necesario actualizarlo aplicando las mejoras identificadas.

Adicionalmente el comité de crisis recibirá los informes de toda incidencia critica que no haya llegado a convertirse en crisis para su evaluación y propuesta de un plan de acción de mejora en aquellos casos que se considere necesario.

Plan de formación y seguimiento

Uno de los elementos clave en la gestión de crisis, es poner constantemente a pruebas los planes y procedimientos diseñados. Para cumplir con este objetivo, se deben poner en marcha iniciativas que permitan evaluar las medidas de actuación que tenemos implementadas frente a situaciones de crisis.

Para poder enfrentarse a una situación de crisis de forma efectiva, es de especial importancia que el equipo se encuentre preparado y entrenado, ya que, para enfrentarse a una situación de estas características, es necesario involucrar a equipos de distinta naturaleza y para que funcionen de forma efectiva en momentos de máxima exigencia deben estar bien preparados.

Para ello, es aconsejable realizar simulacros de distinta tipología, de forma que se someta a sus componentes a las situaciones de gestión que con toda probabilidad una situación de crisis puede dar.

Documento aprobado por dirección