COMPENDIO DE MEJORES PRÁCTICAS SOBRE SEGURIDAD LÓGICA Y FÍSICA DE LAS ENTIDADES ASEGURADORAS

UNESPA.ES

UNESPA

INDICE

[1] El término “Continuidad de Negocio” que se emplea en este Plan de Seguridad y Logística no se refiere a cuestiones relativas a la estrategia de negocio o competitiva de cada entidad, que es una cuestión que deciden y desarrolla cada entidad de forma autónoma e independiente. Se refiere al término técnico adoptado en los estándares internacionales del ISO 22301, que es una norma que establece los requisitos del ciclo de mejora continua (PDCA), en materia de planificación, establecimiento, implantación, operación, supervisión, revisión, prueba, mantenimiento y la mejora de un “Sistema de Continuidad de Negocio” documentado, teniendo en cuenta la gestión de los riesgos globales de cada organización y su capacidad de resiliencia. Se refiere al conjunto de estándares de planificación que acreditan que las organizaciones tienen capacidad de respuesta necesaria para responder a distintos escenarios que se originan en una crisis”

INTRODUCCIÓN

La seguridad, para las entidades aseguradoras adopta una cuádruple dimensión:

- Seguridad física de las personas que han de realizar las labores relacionadas con la actividad aseguradora o ligadas a ella, así como de los clientes o terceros que se encuentren en sus instalaciones o en eventos organizados por la entidad.
- Seguridad de los datos que son confiados a los aseguradores, así como la información de su propiedad sobre la que sustenta su actividad.
- Seguridad relativa a la capacidad de continuar la actividad en situaciones disruptivas externas y no previstas (p. ej., un ciberataque), esto es, la continuidad de los procesos y capital utilizado por cada entidad para llevar a cabo su negocio.
- Como corolario de las tres anteriores, seguridad en la reputación, individual y sectorial, del seguro, como actividad que transmite confianza no sólo a la hora de cumplir sus compromisos, sino en los procesos que instrumenta para realizar dicho cumplimiento.

El presente documento compendia una serie de principios y procesos que constituyen mejores prácticas en materia de seguridad lógica y física, con el objetivo de ayudar a las entidades a mejorar la planificación de riesgos y las medidas para minimizar su impacto. Su contenido está basado en desarrollos y recomendaciones emitidos por instituciones y organizaciones nacionales e internacionales en materia de Seguridad Integral (i.e., de datos, instalaciones, etc., incluyendo Ciberseguridad) y recoge, marcos, posicionamientos y metodologías comunes en este ámbito que puedan ser de interés para el sector asegurador al objeto de que cada entidad pueda adoptar sus propias decisiones de forma autónoma, pero debidamente informada.

PRINCIPIO GENERAL DE PROPORCIONALIDAD

Con carácter general, la gestión de la seguridad lógica y física debe abordarse, por parte de la entidad o grupo asegurador, con proporcionalidad al tamaño, organización interna, naturaleza, ámbito, complejidad y nivel de riesgo de los productos y servicios que provea dicha entidad o grupo o alguna de sus unidades. En tal sentido, este Compendio de Buenas Prácticas, además de tener carácter voluntario, no puede, ni debe, interpretarse como la colección de medidas y procesos que *toda* entidad podría aplicar en *todo* momento; sino como una serie de herramientas que pueden ser utilizadas por cada entidad para, en el marco de su soberanía e independencia de gestión, diseñar su propia estrategia.

CAPÍTULO 1: CONTINUIDAD DE NEGOCIO

DEFINICIÓN DE PLAN DE CONTINUIDAD DE NEGOCIO

PRINCIPIO GENERAL

A los efectos de esta Guía, un Plan de Continuidad de Negocio se entiende como una estrategia estructurada cuyo objetivo es describir las acciones, procesos, responsabilidades y tomas de decisión que se activarán en el caso de que ocurra un suceso que, por sus características intrínsecas, sea susceptible de impedir o limitar la capacidad de la entidad aseguradora de realizar su actividad diaria con normalidad, tanto en los ámbitos de comercialización, como de servicio y prestación o de cualesquiera otros trabajos internos que realice de manera sistemática. Se trata, pues, de un estudio y planificación que supera el ámbito de los planes de contingencia limitados al ámbito de los activos tecnológicos.

COMPENDIO DE MEJORES PRÁCTICAS RELATIVAS AL PLAN DE CONTINUIDAD DE NEGOCIO

- Idealmente, el Plan de Continuidad de Negocio debería incluir entre otras consideraciones:
  - El análisis de impacto de negocio o BIA (de sus siglas en inglés, *Business Impact Analysis*) relativo a la exposición a disrupciones severas en la continuidad de la actividad, teniendo en cuenta el nivel de criticidad de los diferentes procesos y actividades de negocio.
  - La adecuación de la estructura de servicios de tratamiento de la información con los requerimientos de los procesos críticos soportados por dichos servicios.
  - Las medidas tendentes a recuperar los servicios informáticos en caso de un evento que derive en la pérdida total o parcial de dichos servicios; evento comúnmente conocido como "desastre informático".
  - En la medida que la complejidad de la actividad y la criticidad de los procesos así lo justifique, el Plan de Recuperación ante Desastres Informáticos, como integrante del Plan de Continuidad, debería incorporar la definición desde el punto de vista de la actividad de la entidad de, cuando menos, dos parámetros de recuperación:
    - Elemento RTO (o *Recovery Time Objective*), definido como el plazo máximo en el que los sistemas críticos deben ser recuperados (tiempo máximo en el que los sistemas pueden estar fuera de servicio).
    - Elemento RPO (o *Recovery Point Objective*), o tiempo máximo durante el cual es aceptable que una eventual pérdida de datos críticos no se haya subsanado (tiempo máximo entre backups o tiempo máximo de re-trabajo en caso de pérdida de datos).
  - A partir de esta información, el Plan debería incluir escenarios de recuperación y respuesta. De acuerdo con dichos escenarios y el nivel de afección que potencialmente generen sobre la capacidad de negocio de la entidad, se establecerían los correspondientes planes o estrategias de respuesta y recuperación, en los que se describan las acciones para asegurar la integridad, disponibilidad, continuidad y recuperación de los sistemas de la entidad, cuando menos, aquéllos que resulten críticos para su labor. Esta planificación podría incluir las acciones para la continuidad de la actividad en el caso de fallo por parte de proveedores críticos; así como un entorno de contacto y colaboración estrecha entre asegurador y proveedor crítico.
- Es conveniente que estos planes se desarrollen por escrito, trasladando los resultados del BIA al conjunto de los sistemas de información que soportan los procesos de negocio afectados.
- Para que el Plan de Continuidad de Negocio pueda mantener su virtualidad y no caer en la obsolescencia, podrían incorporarse, entre otros, los siguientes elementos:
  - Adaptar su contenido a cualesquiera novedades relevantes en el perfil de la actividad (por ejemplo: ramos de nueva explotación, expansión geográfica, adquisición de carteras, fusiones…).
  - Revisar su contenido con inmediatez a la producción de un suceso negativo que haya comprometido, en todo o en parte, la seguridad de la actividad, o que se considere que, sin haberlo hecho, haya supuesto una amenaza seria a dicha seguridad.
  - Revisar sistemáticamente, con la periodicidad elegida por la entidad, las previsiones del Plan y su eficiencia frente a la realidad de los retos de seguridad experimentados en la actividad.
  - En la medida de lo posible y, sobre todo, cuando la naturaleza y complejidad del negocio así lo aconseje, la entidad podría desarrollar métricas adecuadas para el seguimiento del Plan

de Continuidad de Negocio.

- En cuanto a la gobernanza del Plan de Continuidad de Negocio, se consideran mejores prácticas las siguientes:
  - El nivel de apetito de riesgo de la entidad en materia de seguridad, incluyendo la continuidad de la actividad debería ser aprobado a un nivel decisorio y estratégico adecuado, sin detrimento de que la gestión de los diferentes aspectos de la seguridad pueda ser encomendada a otras unidades, funciones u órganos de la estructura de dicha entidad.
  - Los sucesivos cambios, adiciones y enmiendas del Plan deberían ser conocidos por el órgano decisorio que lo aprobó.
  - Implantar los procesos necesarios para garantizar un flujo adecuado y sistemático de información hacia el órgano decisorio, sobre la marcha y revisiones del Plan de Continuidad de Negocio.
  - Ante sucesos relevantes que afecten a la continuidad del negocio, el órgano decisorio debería poner en marcha las previsiones indicadas en el Plan de Continuidad de Negocio e informar adecuadamente sobre la existencia, características y consecuencias del suceso, así como sobre la puesta en marcha de los procesos indicados en el Plan de Continuidad de Negocio y su eficacia real.
  - El Plan de Continuidad de Negocio debería ser revisado de forma periódica para evitar su obsolescencia. Estas revisiones podrían realizarse anualmente.
  - Es conveniente que las acciones derivadas de la gobernanza del Plan de Continuidad de Negocio estén debidamente documentadas y puestas a disposición de las autoridades de supervisión competentes en los términos que en cada momento fije la legislación.

CAPÍTULO 2: POLÍTICA DE MEDICIÓN DE RIESGOS DE SEGURIDAD LÓGICA Y FÍSICA

MAPEO DE LOS RIESGOS DE SEGURIDAD LÓGICA Y FÍSICA

PRINCIPIO GENERAL
La entidad aseguradora, de forma sistemática y adaptada a la complejidad y naturaleza de su negocio, debería realizar un análisis o mapeo de los riesgos de seguridad física y lógica a los que está sometida.

COMPENDIO DE MEJORES PRÁCTICAS EN MATERIA DE MAPEO DE RIESGOS.

- El mapeo de riesgos debería incluir elementos como:
  - Las actividades y funciones relevantes del negocio.
  - Los activos existentes, incluyendo la interdependencia entre ellos y con los activos de información.
  - Los procesos o servicios que entran en juego, la información o flujo de datos entre los procesos.
- Con carácter general, el análisis de riesgos debería ser suficiente para permitir la definición de los niveles de apetito de riesgo de la entidad.
- La identificación de los riesgos debería permitir clasificarlos en función de su nivel de intensidad o

criticidad (clasificación, al menos, en dos niveles riesgos altos o bajos).

La criticidad sería una combinación entre la probabilidad y el impacto de materialización de los riesgos.

La respuesta definida para cada riesgo podría contener, por ejemplo, las siguientes alternativas:

- Eliminación.
- Mitigación.
- Asunción.
- Transferencia.

Sería deseable que el resultado de este análisis estuviese debidamente documentado.

- Es conveniente actualizar el ejercicio de definición del mapeo, total o parcialmente, con una periodicidad suficiente como para evitar la obsolescencia del ejercicio de diagnóstico. En la medida que la complejidad y naturaleza del negocio de la entidad lo aconsejase, se podrían desarrollar mecanismos destinados a valorar la idoneidad del mapa de riesgos y a proceder, en caso necesario, a su actualización.
- También conviene revisar el contenido y conclusiones del mapa de riesgos tras la producción de un incidente relevante para la seguridad física y lógica de la entidad; con inclusión del análisis de hasta qué punto el mapa de riesgos vigente tuvo en cuenta los riesgos inherentes a dicho incidente, y la forma en la que la estrategia elegida fue, o no, eficiente.
- En la gobernanza del mapa de riesgos es muy conveniente que cada entidad establezca principios claros de referencia; a modo de ejemplo:
  - Informar al órgano decisorio periódicamente sobre los resultados del mapa de riesgos con el objeto de que pueda tomar una decisión informada sobre el nivel de apetito de riesgo aceptado por la entidad.
  - El órgano decisorio, podría encomendar la elaboración y gestión del mapa de riesgos a unidades o funciones de inferior nivel. Sin embargo:
    - Sería informado, con la periodicidad con que se realice el ejercicio de mapeo, de los resultados de éste, a un nivel de granularidad suficiente.
    - Gestionaría los hechos relevantes e incidentes de afección al mapa de riesgos, y supervisaría la adaptación de éste conforme a la experiencia obtenida en dichos hechos.
  - Los resultados del análisis de riesgo podrían ser compartidos con las funciones o departamentos considerados críticos por la entidad, siquiera de forma parcial en lo que dichos riesgos afecten a cada función o departamento; especialmente cuando el ejercicio de mapeo de riesgos exija de estas funciones o departamentos la participación en el ejercicio en sí, esto es, el reporte de sus propias informaciones sobre seguridad lógica y física.
  - En la medida que los resultados del mapa de riesgos revelen una incidencia relevante en el funcionamiento y continuidad de la entidad aseguradora, y/o en la gestión de su caudal de datos personales, la entidad debería tenerlo en cuenta cara a su Autoevaluación de Riesgo y Solvencia. En dicho apartado, la entidad podría explicar someramente el método o métodos adoptados para el mapeo de riesgos de seguridad física y lógica, así como los procesos adoptados para integrar los resultados de dicho ejercicio en su gestión.

- Es conveniente que la gobernanza del mapa de riesgos garantice que, en el marco de este trabajo, se realiza un inventario de los activos relevantes de la entidad relacionados con la seguridad; inventario que podría incluir los niveles de criticidad de dichos activos, así como la identificación de la persona o departamento "propietaria" de dicho activo, en el sentido de ser el responsable de realizar el seguimiento del comportamiento del activo y de su eficiencia en materia de seguridad.

- Una vez realizado el inventario y la clasificación de los activos relevantes, conviene realizar un análisis de los riesgos de seguridad sobre los mismos, y garantizar que los resultados de dicho análisis son consistentes con el apetito de riesgo de la entidad o, en caso contrario, instar la implantación de controles que garanticen dicha consistencia.

➢ En materia de funciones subcontratadas, de acuerdo con el artículo 13.3 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, a los efectos de este Compendio una función subcontratada se define como: «Cualquier tipo de acuerdo celebrado entre una entidad aseguradora o reaseguradora y un tercero, ya sea o no una entidad sujeta a supervisión, en virtud del cual éste, directamente o por subcontratación, realiza una actividad o una función que, en otras circunstancias, hubiese realizado la propia entidad aseguradora o reaseguradora».

- Los proveedores de servicios podrían considerarse función o actividad crítica o importante subcontratada en medida de las dificultades que pudiera generar su disfunción o discontinuidad.

- Los servicios y funciones subcontratados considerados críticos podrían tenerse en cuenta en el mapeo de riesgos de la entidad.

- En todo caso, es conveniente que la entidad se responsabilice de que los proveedores relevantes en materia de sistemas de tratamiento de la información y comunicaciones estén adecuadamente informados de los requerimientos y procesos vigentes en la entidad en materia de seguridad lógica y física.

- En el caso particular de los proveedores en la nube, es conveniente que la entidad, siempre en consistencia con lo que marquen las normas y guías de supervisión en esta materia, diseñe y ejecute los acuerdos de subcontratación de forma que éstos le permitan, en la medida de lo posible, integrar los principios de control y gestión que haya previsto en relación con dichos servicios.

CAPÍTULO 3: CONTROLES DE SEGURIDAD Y VULNERABILIDADES. ESTRATEGIA ICT

PRINCIPIO GENERAL
El ejercicio de mapeo de riesgos define la lista de controles relevantes de seguridad que es necesario implantar para poder enfrentar los riesgos detectados con la estrategia elegida para cada caso. Asimismo, podría disponer de un sistema para la detección de vulnerabilidades y, como consecuencia de todo ello, de una estrategia de seguridad TIC.

COMPENDIO DE MEJORES PRÁCTICAS EN MATERIA DE CONTROLES DE SEGURIDAD Y VULNERABILIDADES, Y ESTRATEGIA TIC

➢ El objetivo de la elaboración de un mapa de riesgos es transmitir una imagen adecuada y precisa de la situación de seguridad de la entidad, y las demandas sobre la misma en esta materia.

- La lista de controles de seguridad y el mapa de riesgos conviene revisarlas en paralelo.
- En la medida que la complejidad y naturaleza del negocio de la entidad lo aconseje, la entidad podría desarrollar métricas para valorar de forma sistemática la idoneidad y eficiencia de los controles de seguridad y revisarlas con la misma periodicidad con que revisa el mapa de riesgos.
- En cuanto al proceso de análisis y detección de vulnerabilidades:
    - Para que sea efectivo debería ser un proceso continuado, sistemático y prudente, en el sentido de incluir todos aquellos activos y elementos de la seguridad lógica de la entidad que no hayan sido revisados periódicamente. A tal efecto, se podrían implantar procesos para la adecuada gestión de estas vulnerabilidades.
    - Incluiría el chequeo de los sistemas de información y los sistemas de seguridad de la información implantados por la entidad, para asegurar su robustez y utilidad, muy especialmente en entornos de modificación en los mismos.
    - Sería conveniente obtener información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la entidad a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
    - Para los casos en los que la vulnerabilidad es detectada por una unidad o función distinta de la que centraliza la política de seguridad lógica y física, debería existir un proceso adecuado para que dicha unidad o función comunique la vulnerabilidad a la función central en el menor tiempo posible.
    - Asimismo, es conveniente que exista un procedimiento establecido para definir las acciones o procesos necesarios para eliminar las debilidades inherentes a la vulnerabilidad. En atención a las características de urgencia en la reacción que pueden llegar a presentar estas situaciones, se debería proporcionar un adecuado nivel de información al órgano decisorio, dependiendo de la importancia del suceso a comunicar.
    - En el marco de los trabajos para la detección de vulnerabilidades, la entidad debería procurar que su personal experto en seguridad lógica participe en el diseño, concepción y realización de los desarrollos de *software*, para poder así garantizar la consistencia de los mismos con el nivel de apetito de riesgo definido.
- Como consecuencia de los resultados del mapeo de riesgos, de la localización de controles y de la detección de vulnerabilidades, la entidad o grupo podría estar en condiciones de elaborar una estrategia de Seguridad ICT (Tecnologías de Información y Comunicación, en sus siglas en inglés), con elementos como:
    - El diseño de la arquitectura de Seguridad ICT elegido por la entidad o grupo.
    - Los objetivos de seguridad marcados.
    - Los planes de acción necesarios para cumplir estos objetivos.
    - La planificación de la evolución de la estrategia, así como los procesos de chequeo y auditoría de la misma.
    - Las acciones a llevar a cabo en relación con terceros proveedores y servicios subcontratados.
    - También podría formar parte del sistema de seguridad o estrategia de Seguridad ICT la implantación de un proceso de cambio, Este proceso garantizaría que las modificaciones en los sistemas de Seguridad ICT son debidamente valoradas, chequeadas, aprobadas e implantadas, incluyendo, por ejemplo, las adecuadas rutinas de autorización para la puesta

en producción de los nuevos sistemas o equipamientos.

- En el marco de la gobernanza de la seguridad lógica y física, la entidad o grupo conviene definir qué unidad, función, departamento o similar dentro de su estructura se responsabilizaría del control y gestión de la Estrategia de Seguridad ICT. El órgano decisorio asumiría la aprobación de la estrategia de seguridad, y la comprobación de que existen los procesos necesarios para recibir información adecuada sobre la gestión de la Estrategia de Seguridad ICT.
- Son funciones habituales de la gestión de la Estrategia de Seguridad ICT:
  - La determinación del nivel de apetito de riesgo para cada uno de los controles o riesgos de seguridad, en coherencia con el apetito general de riesgo definido por la entidad.
  - La identificación constante de los riesgos a los que está efectivamente expuesta la entidad o grupo.
  - La definición de medidas de mitigación y control, cuando esto sea necesario por no haber sido definido en algún escalón previo (mapa de riesgos, detección de controles, etc.)
  - La monitorización de la efectividad de las medidas implantadas.
  - El reporte sobre todo ello al órgano decisorio adecuado.
- Siempre de forma proporcional a la naturaleza y escala de su actividad, conviene que la entidad disponga, dentro de su estructura corporativa, de una función encomendada de la Seguridad ICT, con adecuados niveles de autonomía y capacidad de reporte.
- Esta función podría estar separada de los procesos de operación de los activos ICT, y reportar al máximo nivel de gestión.
- La entidad o grupo podría activar una labor o función de auditoría de la Estrategia de Seguridad ICT, con suficientes niveles de independencia para revisar, desde un punto de vista basado en riesgo, el cumplimiento de las actividades relacionadas con la Estrategia de Seguridad ICT y su consistencia con la operativa general de la entidad o grupo.
- La estrategia de seguridad así definida debería tener establecida una rutina de chequeo y comprobación de los sistemas de información desde el punto de vista de la seguridad, especialmente en los momentos en que dichos sistemas están siendo objeto de modificaciones relevantes.

CAPÍTULO 4: SEGURIDAD DE LA INFORMACIÓN

PRINCIPIO GENERAL

En proporción a la naturaleza y escala de su actividad, conviene que la entidad o grupo asegurador defina los principios de alto nivel de su política de seguridad en la información, con el objetivo de proteger la confidencialidad, la integridad y la disponibilidad de los datos en su poder.

COMPENDIO DE MEJORES PRÁCTICAS EN MATERIA DE SEGURIDAD EN LA INFORMACIÓN

- Estos principios podrían incluir:
  - Una descripción de las principales responsabilidades en la gestión de la seguridad en la información.
  - Los requerimientos para el personal y para terceros, los procesos y la tecnología necesarios para garantizar dicha seguridad.

- Las garantías de confidencialidad, integridad y disponibilidad de los activos físicos y lógicos de carácter crítico de la entidad, así como de sus datos sensibles y, en todo caso, aquellos datos o conjuntos de datos cuya especial protección se defina en las normas.
- La identificación de vulnerabilidades.
- La comprobación de que el *software* utilizado es adecuado y está debidamente actualizado.
- La implantación de las adecuadas medidas de seguridad para los equipos, eventualmente medidas de encriptado y similares.
- Seguridad en las conexiones de otros aparatos (ordenadores, móviles, etc.) con los activos ICT de la entidad.
- Integridad de los activos ICT.
- La estrategia de Seguridad ICT conviene que se concrete en una operativa ICT, sistemática y adecuadamente descrita, por la cual se llevarán a cabo las labores y rutinas necesarias para cumplir con los objetivos de la estrategia ICT definida. Esta operativa podría incluir elementos como:
    - El control y notaría de procedimientos relacionados con operaciones ICT de carácter crítico.
    - Inventario actualizado de los activos ICT.
    - Control y gestión del ciclo de vida de los activos ICT.
    - Control de que dichos activos ICT mantienen la capacidad necesaria.
    - Sistemas de backup o restauración de datos; etc.
- Más concretamente, conviene establecer un proceso que gestione la adquisición, desarrollo y mantenimiento de los sistemas ICT, que garantice su adecuada implementación y funcionamiento e que incluya los chequeos necesarios y los estándares de seguridad. Estos procesos deberían ser garantes de que los activos adquiridos son coherentes con los objetivos de la estrategia de Seguridad ICT, y podrían proteger el proceso de implantación, desarrollo y mantenimiento frente a manipulaciones u otras vulnerabilidades. Estos procesos también podrían abarcar a aquellos activos ICT usados por funciones del negocio fuera de la estructura de la propia entidad.
- La entidad o grupo debería definir y documentar procedimientos para el control del acceso lógico. Esto supondría garantizar a los usuarios de los sistemas el acceso mínimo para realizar sus tareas estableciendo controles para los diferentes niveles de permiso y para gestionar esos accesos.
- Conviene revisar periódicamente la política de permisos para evitar que personas sigan disponiendo de accesos que ya no necesitan o para los que ya no están autorizados.
- Las medidas de seguridad lógica podrían incluir elementos como:
    - La limitación del uso de cuentas de usuario genéricas o compartidas.
    - La limitación de los accesos con privilegios altos o totales.
    - Procesos robustos para el control del acceso remoto.
    - Sistemas de notaría o log de los accesos producidos.

- Procedimientos de autenticación.
- En todo caso, estas políticas podrían revisarse periódicamente para garantizar que siguen siendo adecuadas al perfil y a las necesidades de la actividad.

- Seguridad física: La entidad o grupo debería definir e implantar medidas de seguridad que protejan sus instalaciones, o partes de ellas especialmente sensibles, del acceso no autorizado. Esto debería tener como uno de los objetivos prioritarios los sistemas de información. El esquema básico de la protección ante la intrusión pasa por el planteamiento y el estudio de los objetivos, los medios técnicos y las medidas organizativas. Los sistemas de acceso físico se deberían revisar periódicamente.

- Incidentes: Dentro de su política de seguridad de la información, la entidad o grupo conviene disponer de un procedimiento para la gestión de incidentes. Dicho procedimiento podría establecer, entre otros, los siguientes aspectos:

  - Los procedimientos necesarios para rastrear, registrar y clasificar los incidentes de acuerdo con su nivel crítico.
  - Las responsabilidades en diferentes tipos de eventos.
  - Los procedimientos que se usarán para identificar, analizar y reparar la causa primera del incidente.
  - La política de comunicación interna de estos incidentes y, eventualmente, de comunicación externa.
  - En la medida en que dicha definición sea posible, los procedimientos que se activarán para mitigar las consecuencias del suceso.
  - Los mecanismos para permitir localizar y gestionar los tipos, volúmenes y costes de los incidentes en la seguridad de la información.
  - Los procesos necesarios para la correcta vigilancia y gestión del incidente, con el objetivo de identificar las causas del mismo y actuar contra ellas.
  - Proceso para clasificar los incidentes de acuerdo con su criticidad, generando con ello diferentes protocolos de actuación.
  - Procedimientos necesarios para dar adecuada respuesta a las obligaciones de comunicación de incidentes que en cada momento fije la legislación de aplicación.

- La entidad debería procurar que sus trabajadores estén adecuadamente formados e informados en materia de seguridad, de manera que posibiliten la protección de la entidad frente a riesgos de esta naturaleza. Estas políticas de formación e información podrían aplicarse con determinada periodicidad.

CAPÍTULO 5: OTROS ASPECTOS DE LA GOBERNANZA DE LA SEGURIDAD LÓGICA Y FÍSICA

PRINCIPIO GENERAL

Dado que la complejidad y naturaleza de la actividad aseguradora puede ser muy variada, la entidad debería determinar qué departamento(s) o función(es) han de implicarse en la gestión diaria de la seguridad lógica y física de la entidad, de acuerdo con el nivel de apetito de riesgo definido.

COMPENDIO DE MEJORES PRÁCTICAS EN MATERIA DE GOBERNANZA DE LA SEGURIDAD LÓGICA Y FÍSICA

- Se consideran como mejores prácticas las siguientes:
  - La existencia de una unidad o función que centralice toda la información relativa a la seguridad lógica y física, y su gestión independientemente del número de departamentos o funciones que participen en la gestión de la seguridad lógica y física de la entidad, o del nivel de unidades de decisión geográficas de que disponga la entidad.
  - El establecimiento de un procedimiento, suficientemente conocido por la organización, relativo a hechos relevantes para la seguridad lógica y física de la entidad, en el que queden definidas las responsabilidades de reporte, análisis y actuación de cada una de las partes implicadas, y que garantice una gestión coordinada de dichos hechos relevantes.
  - La adecuada integración en los objetivos, estrategia y gestión de la entidad aseguradora, de los servicios o funciones subcontratados.
- En todo caso, conviene que el órgano de decisión sea el responsable último del diseño, mantenimiento, chequeo, reforma y modificación de los procesos y análisis relacionados con la seguridad lógica y física, así como de la estrategia de seguridad adoptada.
- El órgano de decisión también velaría porque las personas a cargo de las diferentes labores relacionadas con los mismos tienen la cualificación adecuada; así como de que la adecuada gestión de las labores y necesidades aquí descritas dispongan de una adecuada dotación presupuestaria dentro de las disponibilidades de la entidad.
- En aquellos casos en los que la legislación relevante (de seguridad, protección de datos, etc.) establezca la obligación de disponer de un interlocutor o gestor centralizado, conviene que las entidades valoren desarrollar y poner en marcha dichas figuras.
  - Idealmente sería el órgano de decisión el responsable último de que la entidad o grupo defina, de forma clara, los roles y responsabilidades en materia de seguridad lógica y física en el ámbito de la entidad o grupo. La forma de organizar la seguridad ha de estar claramente definida y adecuadamente comunicada a todas las partes implicadas.
  - A los efectos de este documento una situación de crisis es todo aquel acontecimiento relevante que, o bien genere una disrupción en la actividad de la entidad aseguradora, o bien tenga la clara potencialidad de generarla.

    Se consideran como buenas prácticas las siguientes:

    - Existencia de un procedimiento general establecido para situaciones de crisis, expresado por escrito y suficientemente conocido por todas las partes implicadas en el mismo. Este

procedimiento podrá, según el criterio de la entidad, formar o no parte del Plan de Continuidad de Actividad.

- Establecimiento de una disciplina de decisiones clara y taxativa por la que se regirá el procedimiento de situaciones de crisis.
- Inclusión de políticas adecuadas de comunicación interna relacionadas con el suceso; así como externas, en los casos en los que dicha comunicación sea relevante o necesaria.