POLÍTICA DE CONTINUIDAD DE NEGOCIO

Índice

La presente Política ha sido analizada y su propuesta ha sido aprobada por el Comité de Dirección, por el Comité de Riesgos, proponiendo el visto bueno por la Comisión de Auditoría con carácter previo a su presentación y aprobación por el Consejo de Administración.

Es un documento para uso exclusivo de SegurCaixa Adeslas, S.A. de Seguros y Reaseguros (en adelante también, "SCA", "la Compañía" o "la Entidad").

Política de Continuidad de Negocio

Fecha de aprobación:	18 de Diciembre de 2024
Responsable de edición y revisión	D. Seguridad Digital y Continuidad

Registro de revisiones

Las diferentes revisiones del presente documento serán anotadas en este registro, incluyendo el número de versión, fecha de publicación, tipo de revisión y los responsables de su aprobación y revisión:

Versión	Fecha	Modificaciones	Revisado Por	Aprobado Por
01	16/12/2015	Edición	DA Organización y Calidad	Consejo de Administración
02	21/02/2018	Modificación	DA Organización y Calidad	Consejo de Administración
03	17/10/2019	Modificación	D. Organización y RRHH	Consejo de Administración
04	16/10/2020	Modificación	D. Organización y RRHH	Consejo de Administración
05	16/12/2021	Modificación	D.A. Seguridad Digital y Continuidad	Consejo de Administración
06	14/12/2022	Modificación	D.A Seguridad Digital y Continuidad	Consejo de Administración
07	14/12/2023	Modificación	D.A. Seguridad Digital y Continuidad	Consejo de Administración
08	18/12/2024	Modificación	D. Seguridad Digital y Continuidad	Consejo de Administración

La revisión de esta Política ha sido realizada por:

- Dirección de Seguridad Digital y Continuidad: ha supervisado la realidad y desarrollo de los procesos que comprende esta Política y que se recogen los elementos necesarios para la implementación de la misma dentro de la organización, en el ámbito que le compete.
- Dirección de Infraestructura y Arquitectura: ha supervisado la realidad y desarrollo de los procesos que comprende esta Política y que se recogen los elementos necesarios para la implementación de la misma dentro de la organización, en el ámbito que le compete.
- Dirección de Tecnología y Transformación Tecnológica: ha supervisado la realidad y desarrollo de los procesos que comprende esta Política y que esta recoge los elementos necesarios para la implementación de la misma dentro de la organización, en el ámbito que le compete.

- Dirección de Control de Riesgos: ha supervisado la coherencia de esta Política con el resto de Políticas que conforman el sistema de gobierno de SegurCaixa Adeslas.
- Función de Verificación del Cumplimiento: ha verificado que esta Política contiene todos los elementos fundamentales que son requeridos por la normativa vigente que le aplica.

1. Introducción

La presente Política se enmarca en el Sistema de Gobierno y de gestión de riesgos establecido por SegurCaixa Adeslas. Los aspectos comunes y generales que definen el marco del Sistema de Gobierno se encuentran recogidos en la Política de Gestión de Riesgos. Por tanto, en esta política se incluyen sólo aquellos aspectos específicos a la misma.

En consecuencia, el capítulo de Introducción de la Política marco de Gestión de Riesgos, (antecedentes, ámbito de aplicación, entrada en vigor, cláusula de actualización y requerimientos a nivel de Grupo), será de aplicación a la presente Política y, en caso de documentación separada de la misma deberá incorporarse dicho contenido como parte integrante de esta Política.

1.1. Antecedentes

El Reglamento Delegado 2015/35, en su artículo número 258, establece que las empresas de seguros y reaseguros establecerán, aplicarán y mantendrán una política de continuidad de las actividades dirigida a garantizar que, en caso de sufrir alguna interrupción en sus sistemas y procedimientos, se preserven los datos y funciones esenciales y se mantengan las actividades de seguro y reaseguro o, de no ser posible, que tales datos y funciones se recuperen oportunamente y sus actividades de seguro o reaseguro, se reanuden oportunamente.

A lo anterior es necesario unir la aprobación y entrada en aplicación del *Reglamento (UE) 2022/2554, de 14 de diciembre sobre resiliencia operativa digital del sector financiero* (en lo sucesivo también Reglamento Delegado 2022/2554 o por su acrónimo en ingles Reglamento DORA), que tiene como objeto consolidar y actualizar los requerimientos relativos al riesgo relacionado con las TIC como parte de los requisitos en materia de riesgo operativo que se han venido abordando hasta su fecha de forma separada por la normativa específica que regula cada tipología de entidad financiera, y donde se recoge requerimientos adicionales en materia TIC a considerar en sus Políticas de Continuidad.

De forma adicional, existen otras normas, directrices y prácticas de mercado que establecen requerimientos y recomendaciones para la gestión del riesgo tecnológico y de seguridad de la información. Esta normativa específica, está recogida en el Anexo de la Política”

Esta política está debidamente adaptada a los principales requerimientos establecidos en las normas anteriores y se adapta y recoge las mejores prácticas en esta materia, así como a las recomendaciones recibidas de los accionistas.

1.2. Objetivo de la Política

El objetivo de la presente Política, es establecer el marco general que es necesario, con sus principios y características generales, así como regular los aspectos dotacionales y técnicos, que permitan garantizar la implantación y operación de un Sistema de Gestión de Continuidad de Negocio, (en adelante “SGCN” o “el Sistema”), eficaz.

SCA ha procedido a redactar esta Política con el fin de mantener un SGCN operando, en ciclo de mejora continua, que permita la consecución de los siguientes objetivos principales:

- Determinar el sistema de gobierno relativo al SGCN que permita una gestión y supervisión integral de todos sus componentes organizativos, operativos, tecnológicos y de comunicación.

- Identificar los Riesgos de resiliencia operativa y continuidad de Negocio de SCA.
- Mitigar estos riesgos, implantando estrategias de recuperación de activos críticos que permitan la continuidad de los servicios prestados a nuestros clientes, en el menor tiempo posible, tras una interrupción.
- Mejorar de forma continua el sistema, incrementando sus niveles de eficiencia y eficacia.
- La interrelación entre continuidad de la actividad en sentido global y la continuidad de la actividad en materia TIC

Asimismo, y acorde a los puntos expresados anteriormente, el SGCN implantado en SCA, en base a esta Política, asume el cumplimiento de los siguientes objetivos adicionales:

1. Velar por la protección de sus empleados, personal externo, proveedores y cualquier persona presente o que preste servicios en sus instalaciones, en caso de que una contingencia afecte a dichas instalaciones.

2. Proporcionar sus servicios a sus clientes dentro de los parámetros de tiempo, forma y calidad mínimos exigidos y previamente acordados, garantizando a su vez, la vuelta a la normalidad de todas las actividades causando la menor repercusión posible en todos los grupos de interés.

3. Incorporar la función de continuidad de negocio como una función más dentro de la cultura empresarial de SCA.

4. Velar por la reputación e imagen de marca de SCA.

Con la finalidad de cumplir con los objetivos expuestos en esta Política, se establecen los siguientes principios a través de los cuales SCA, se compromete a desarrollar la actividad indicada por la misma:

1. **Principio de Garantía**, proporcionando todos los medios económicos y logísticos para la constitución, implantación, mantenimiento y evolución del Sistema de Gestión de Continuidad de Negocio y sus actividades asociadas.

2. **Principio de Concienciación**, apoyando la promoción, conocimiento y concienciación en Continuidad de Negocio entre sus empleados.

3. **Principio de implantación y mantenimiento**, facilitando la implantación y dotación del SGCN, así como velando por el mantenimiento del mismo.

4. **Principio de Verificación**, realizando pruebas periódicas necesarias para contrastar el correcto funcionamiento de los planes a la par que instruir a los grupos técnicos y de negocio involucrados en las actividades de continuidad de negocio.

5. **Principio de Mejora Continua**, estableciendo la necesidad y compromiso de realizar la mejora y evolución continúa del SGCN, acondicionándose a los cambios tanto internos como externos.

6. **Principio de Coordinación y Responsabilidad,** definiendo e implantando las herramientas de colaboración y comunicación entre las diferentes funciones y direcciones involucradas y garantizando el compromiso de todas y cada una de ellas en la consecución de los objetivos del SGCN.

2. Gobernanza, Funciones y Responsabilidades

Con objeto de operar esta Política, así como reportar y comunicar periódicamente el estado de la continuidad de negocio en SegurCaixa Adeslas, se definen las determinadas obligaciones y responsabilidades, para las diferentes áreas de la Organización en relación con la gestión del SGCN:

2.1. Consejo de Administración.

El Consejo de Administración es responsable de los siguientes aspectos relacionados con el SGCN:

- Aprobar, supervisar y revisar como parte de sus requisitos generales de gobernanza la presente política Continuidad de Negocio que incluirá las medidas de continuidad TIC (entre ellas la aplicación de los planes de respuesta y recuperación en materia TIC), garantizando que la misma es revisada periódicamente y cuando se produzcan cambios significativos que afecten a sus contenidos, dando las indicaciones oportunas para su divulgación en la organización, así como a terceras partes interesadas cuando se estime pertinente.
- Establecer el perfil y las estrategias de gestión de los riesgos de resiliencia operativa y continuidad de negocio de acuerdo con lo establecido en la Política de Gestión de Riesgos y en los términos de esta política.
- Aprobar los límites cuantitativos que ayuden a definir el nivel de apetito al riesgo. Los límites y niveles de apetito se recogen en la política de gestión de riesgos.
- Asegurarse de la existencia de recursos humanos, técnicos y económicos adecuados y suficientes para garantizar su correcto funcionamiento y el liderazgo que lleve a contemplar esta política como parte de la cultura de SCA y su estrategia.
- Ser informado, y adoptar las decisiones oportunas, sobre cualquier incidente o hecho relevante que afecte severamente a la continuidad de negocio, así como cualquier hecho o circunstancia relevante que se presente en relación a esta política que sea trasladada por el Comité de Dirección.
- Tomar conocimiento de los resultados de las deficiencias identificadas como resultado de las pruebas realizadas sobre los Planes de Continuidad de Negocio.
- Mantenerse informado, a través de la Comisión de Auditoría, del Informe anual de Continuidad de negocio.

2.2. Comisión de Auditoría

- Supervisar la eficacia del control interno, la auditoría interna y los sistemas de gestión de riesgos de la entidad, incluyendo los riesgos de continuidad de negocio.
- Analizar, con carácter previo a su presentación en el Consejo de Administración, cualquier incidente o hecho relevante que afecte severamente a la continuidad de negocio, así como cualquier hecho o circunstancia relevante que se presente en relación a esta política que sea trasladada por el Comité de Dirección.

- Se le informará sobre el Informe Anual de Continuidad de Negocio y Resiliencia TI.
- Analizar e informar sobre la propuesta relativa a los indicadores de Apetito por el Riesgo y el cumplimiento de sus límites conforme a lo establecido en la Política de Gestión de Riesgos.

2.3. Comité Transformación Tecnológica

- Aprobación del procedimiento de Continuidad TI y las propuestas de los planes de respuesta y recuperación.

2.4. Comité de Riesgos

- Supervisará el Informe Anual de Continuidad de Negocio y Resiliencia TI y en particular sobre los siguientes aspectos:
  - Análisis de impacto (BIAs), así como de los riesgos de Resiliencia TI y Continuidad de Negocio.
  - Resultados de los Planes de Recuperación de Desastre o “Disaster Recovery Plans”, (DRPs).
  - Seguimiento de los indicadores de riesgo y métricas de desempeño de Continuidad de Negocio y Resiliencia TI.
  - Resultados del proceso de autoevaluación de riesgos y controles relacionados con la resiliencia operativa y la continuidad de negocio, y si procede, los resultados alcanzados en la evaluación de escenarios de riesgo operacional.
- Supervisará con carácter previo a su presentación en la Comisión de Auditoría y el Consejo de Administración, cualquier incidente o hecho relevante que afecte seriamente a la continuidad de negocio, así como cualquier hecho o circunstancia relevante que se presente en relación a esta política que sea trasladada por el Comité de Dirección.
- Revisar la propuesta de los límites de apetito al riesgo y realizar el seguimiento del cumplimiento de los límites conforme a lo establecido en la Política de Gestión de Riesgos.

2.5. Comité de Dirección

El Comité de Dirección, presidido por el Director General, es responsable de adoptar dentro de la organización, las medidas técnicas, organizativas y de control que garanticen la operación de la Política de Continuidad de Negocio y de la implementación de una cultura de continuidad.

Sus responsabilidades se concretan en las siguientes tareas:

- Es el responsable de definir las líneas de gestión de la continuidad de negocio, en línea con las directrices y estrategia establecidas por el Consejo de Administración y para ello, de aprobar el diseño, dotación y el dimensionamiento del SGCN; asegurándose de su adecuado funcionamiento.

- Es responsable de la implementación de los procedimientos de gestión de riesgos en línea con las directrices establecidas por el Consejo de Administración y de diseñar y operar una estructura organizativa que permita la adecuada aplicación y desarrollo del Sistema de Gestión de Continuidad de Negocio y en ese sentido:
  - Supervisará los incidentes de continuidad sobre cualquier activo crítico que se consideren relevantes por parte del Comité de Continuidad de Negocio y Resiliencia TI.
  - Deberá permanecer involucrado en la actividad del SGCN analizando el Informe Anual de Continuidad de Negocio y Resiliencia TI.
  - Revisará los resultados de las pruebas realizadas sobre los Planes de Continuidad de Negocio y las deficiencias identificadas, así como aquellas modificaciones relevantes del SGCN que le sean notificadas.
  - Comunicará al Consejo de Administración cualquier hecho o circunstancia relevante que se presente en relación a esta política.

2.6. Comité de Continuidad de Negocio y Resiliencia TI

Está integrado por dos tipos de miembros, que se diferencian entre sí por su grado de involucración y potestades:

Miembros Permanentes: Constituyen el núcleo del Comité y deben asistir a todas sus convocatorias.

Tienen la potestad de invitar a los Miembros Consultivos y al resto de personal que estimen necesario para la documentación, asesoramiento y operación de las tareas a realizar por el Comité.

Son los que se detallan a continuación:

- El Director de Seguridad Digital y Continuidad, (en adelante “Chief Information Security Officer” o por su acrónimo “CISO”), que presidirá el Comité.
- El Director de Tecnología y Transformación Tecnológica.
- Director de Negocio
- Director de Servicio al Cliente
- El Director de Infraestructura y Arquitectura
- El Director de Organización y RRHH,
- El Director de Control de Riesgos.
- El Director de Marketing
- El Director de Comunicación.
- El Director de Compras

- El Responsable de Gobierno, Riesgo y Cumplimiento de Seguridad Digital.
- El Responsable de Continuidad de Negocio y Resiliencia TI que actuará como secretario del Comité.

Miembros Consultivos: Son aquellos titulares de subdirecciones o áreas de relevancia en la compañía, que pueden ser convocados a Comité en función de los asuntos a tratar.

Deben asistir a todas las convocatorias a las que se les invite por indicación de algún miembro permanente.

Son los que se detallan a continuación:

- El Director Económico Financiero, Control de Gestión y Control de Riesgos.
- El Director de Secretaria General.
- El Director de Desarrollo Corporativo.
- El Delegado de Protección de Datos Personales.

El Comité de Continuidad de Negocio y Resiliencia TI y por extensión, sus miembros, son los responsables de:

- Establecer los mecanismos de comunicación internos que garanticen que todo el personal relevante de la organización y terceras partes interesadas, estén familiarizados y cumplan con el contenido de esta Política, en sus respectivos ámbitos de responsabilidad.
- Encomendar a las unidades organizativas, operativas y de soporte, la responsabilidad del diseño, implantación y control del Sistema de Gestión de Continuidad de Negocio, bajo los criterios y parámetros establecidos por el Consejo de Administración en los procesos, actividades y riesgos de los que sean propietarios, sin perjuicio de la existencia de unidades específicas encargadas de la supervisión y control de los mismos.
- Aprobar formalmente y velar por la implementación de los manuales y procedimientos definidos en el SGCN de SCA, así como de cualquier actualización de los mismos velando que sean completos y estén operativos.
- Aprobar los presupuestos del SGCN, de sus planes de formación y concienciación establecidos y garantizar su ejecución.
- Supervisar los Planes de Continuidad y Resiliencia TI, donde se desarrollen las diferentes estrategias y procedimientos de recuperación ante incidentes de continuidad de negocio velando por el cumplimiento correcto de las medidas establecidas en el SGCN durante la gestión de los mismos. Estos Planes y sus documentos asociados, serán actualizados al menos una vez al año para soportar de forma permanente la continuidad de las actividades de SCA divulgándolos entre las partes involucradas con algún tipo de responsabilidad o interés.
- Analizar los resultados de los análisis de impacto de negocio (“Business Impact Analysis” o “BIAs”).
- Analizar los resultados de las Pruebas sobre los Planes de Recuperación de Desastre o “Disaster Recovery Plans”, (DRPs).

- Evaluar los incidentes de Seguridad Digital que puedan afectar a la continuidad de negocio que le sean escalados por el Comité de Seguridad Digital tal y como establece la Política de gestión y control del riesgo tecnológico y la Política de seguridad de la información.

- En caso de un incidente de cualquier activo crítico con impacto en la continuidad de las actividades de SCA, a petición del CISO, se declarará la activación del plan de contingencia y la dirección y coordinación de la puesta en marcha de los Planes de Continuidad de negocio y Resiliencia TI aprobados y realización de las convocatorias del Equipo de Gestión de Incidentes, (EGI), según el manual de gestión de incidentes y crisis, si tras la evaluación del impacto y las consecuencias, ello fuera necesario.

- Gestionar la resolución de las crisis en la entidad estableciendo, entre otros, procedimientos claros para gestionar las comunicaciones de crisis internas y externas.

- Realizar el seguimiento de indicadores de riesgo y métricas de desempeño de Continuidad de Negocio y Resiliencia TI.

- Aprobar el Informe Anual de Continuidad de Negocio y Resiliencia TI en SCA, que incluirá en su caso aquellos cambios necesarios a introducir sobre el SGCN.

- En el ámbito específico de la Resiliencia TI tendrá adicionalmente las siguientes responsabilidades:

    - Reportar y comunicar aquellas prácticas desplegadas con el objetivo de fortalecer los aspectos de Resiliencia TI relacionados con la recuperación ante Incidentes de Seguridad.

    - Supervisar los Planes de Continuidad y Resiliencia TI, dónde se desarrollen las diferentes estrategias y procedimientos de recuperación ante incidentes de continuidad de negocio velando por el cumplimiento correcto de las medidas establecidas en el SGCN durante la gestión de los mismos. Estos Planes y sus documentos asociados, serán actualizados al menos una vez al año para soportar de forma permanente la continuidad de las actividades de SCA divulgándolos entre las partes involucradas con algún tipo de responsabilidad o interés. Solucionar riesgos y bloqueos existentes sobre tecnología, proveedores u otras dependencias que impidan la consecución de los objetivos definidos por negocio ante una disrupción del mismo, desde el punto de vista de disponibilidad.

    - Verificar el estado de las iniciativas de Resiliencia TI necesarias para garantizar el establecimiento de la función en SegurCaixa Adeslas: formación y concienciación, fortalecimiento del Modelo de Gobierno de Resiliencia desplegado, evolución de la resiliencia en los activos críticos, reducción de la obsolescencia y, la definición y puesta en marcha del modelo de mejora continua, entre otros.

Sin menoscabo de su supervisión formal por el Comité de Riesgos, el Comité de Continuidad de Negocio y Resiliencia TI debe validar los siguientes aspectos:

- El análisis y supervisión de los riesgos relacionados con la resiliencia operativa y la continuidad de negocio, así como las estrategias de continuidad gestionadas por la D. Seguridad Digital y Continuidad.

- El Plan de Pruebas sobre los Planes de Continuidad y Resiliencia TI aprobados y la supervisión de los resultados de las mismas y de los planes de acción establecidos haciendo énfasis en los resultados de las Pruebas sobre los Planes de Recuperación de Desastre o “Disaster Recovery Plans”, (DRPs).

- Realizar la propuesta de los niveles de apetito al riesgo de los riesgos de Continuidad de Negocio y Resiliencia TI y evaluar su cumplimiento conforme a lo establecido en la Política de Gestión de Riesgos.

2.7. Dirección de Seguridad Digital y Continuidad

La gestión de la Continuidad de Negocio y Resiliencia TI es desempeñada por la Dirección de Seguridad Digital y Continuidad, dependiente de la Dirección de Tecnología y Transformación Tecnológica.

Es responsabilidad de la Dirección de. Seguridad Digital y Continuidad, la gestión de esta Política y de la interpretación de dudas que puedan surgir en su aplicación junto con la Dirección de Control de Riesgos.

Del mismo modo, sus cometidos son los que a continuación se relacionan:

- Apoyar al Consejo de Administración a definir y mantener la Política de Continuidad de Negocio y controlar su implantación y difusión.

- Informar al Consejo de Administración, periódicamente y en momentos puntuales, sobre los resultados de los procesos de gestión de los riesgos de resiliencia operativa y continuidad de negocio y su evolución.

- Actuar como órgano asesor del Comité de Dirección, en relación a la Continuidad de Negocio sobre la base de las responsabilidades que se le atribuyen en esta política.

- Propondrá los presupuestos del SGCN, de sus planes de formación y concienciación establecidos y garantizar su ejecución.

- Establecer los Planes de Continuidad y Resiliencia TI, dónde se desarrollen las diferentes estrategias y procedimientos de recuperación ante incidentes de continuidad de negocio y resiliencia TI velando por el cumplimiento correcto de las medidas establecidas en el SGCN durante la gestión de los mismos.

- Definir, implantar y mantener actualizados los procesos y procedimientos establecidos en el SGCN, gestionando para ello, la dotación técnica, humana y presupuestaria, asignada. La actualización del SGCN se hará con un enfoque de mejora continua, que permita la minimización de los riesgos de resiliencia operativa y continuidad de negocio en los activos críticos identificados.

- Informar a la Dirección de Control de Riesgos sobre el modelo de gestión de los riesgos de resiliencia operativa y continuidad de negocio, así como de los mecanismos de gobernanza y control interno del SGCN

- Se coordinará con la Dirección de Infraestructura y Arquitectura, la Dirección de Organización y RRHH y La Dirección de Compras para asegurar que todos los activos críticos de SCA, (Personas, Proveedores, Sedes y Sistemas), contemplen los requisitos del SGCN.

- Definir conjuntamente con la Dirección de Control de Riesgos los indicadores de riesgo y métricas de desempeño de Continuidad de Negocio y Resiliencia TI, y determinar aquellos que se incorporarán al Marco de Apetito al riesgo.
- Realizar los análisis de impacto, (BIA) y comunicar internamente las variaciones en los requisitos de disponibilidad de recursos técnicos originados en las áreas de Negocio.
- Realizar el análisis y evaluación de los riesgos de resiliencia operativa y continuidad de negocio relacionados con los activos críticos Personas, Sedes, Proveedores y Sistemas de Información, estableciendo y evaluando los controles y medidas para su adecuada gestión y mitigación en coordinación con las áreas afectadas y la Dirección de Control de Riesgos.
- Sobre los Planes de Continuidad y ResilienciaTI, definirá los Planes de Recuperación de Desastre o “Disaster Recovery Plans”, (DRPs), y Planes de Contingencia, dando respuesta a los escenarios desastre a los que, tras analizarlo, se pueda ver expuesto la organización.
- Establecer y dar cumplimiento, conjuntamente con las unidades operativas a los planes de pruebas.
- Gestionar los incidentes que afecten a la continuidad de negocio de acuerdo a lo establecido en los procesos y procedimientos establecidos en el SGCN y adicionalmente, valorando la efectividad de estos procedimientos, la rapidez de respuesta ante alertas y su determinación de impacto, así como la efectividad del escalado del incidente, de sus comunicaciones, etc.
- Con posterioridad a dichos incidentes, deberá generar, valorar y comunicar, los análisis forenses apropiados para cumplir con los requisitos anteriores.
- En el ámbito específico de la Resiliencia TI será responsable de las tareas atribuidas en la Política de gestión y control del riesgo tecnológico y la Política de seguridad de la información.
- Coordinar el reporte en el Comité de Continuidad de Negocio y Resiliencia TI sobre el estado de la continuidad de negocio y resiliencia TI en SCA sobre la base de las responsabilidades que se atribuyen al mismo en esta política.
- Mantener un registro de los incidentes con afectación a la continuidad en SCA.

Con el objetivo de informar anualmente de todo lo anterior, y en general sobre el SGCN, elaborará un Informe Anual de Continuidad de Negocio y Resiliencia TI de SCA y lo someterá a la aprobación del Comité de Continuidad de Negocio y Resiliencia TI.

2.8. Dirección de Infraestructura y Arquitectura

La Dirección de Infraestructura y Arquitectura, en coordinación y supervisión por la Dirección de Control de Riesgos y la Dirección de Tecnología y Transformación Tecnológica, es el área responsable implantar las medidas técnicas que el SGCN en la parte que se refiere a la disponibilidad de los activos críticos Datos y Sistemas, y en concreto:

Con el objeto de garantizar la resiliencia de los activos críticos anteriores, implementará los requisitos establecidos en los Planes de Recuperación de Desastre o “Disaster Recovery Plans”, (DRPs), y en particular:

- Define y mantiene el catálogo de recursos tecnológicos asignados a procesos de negocio (CMDB) consistente con el BIA y la estrategia definida del SGCN.
- Comunica a la mayor brevedad posible, las posibles incidencias que detecte en los sistemas y comunicaciones con objeto de activar y/o predisponer los mecanismos y acciones previstos en el Sistema de Continuidad de Negocio.
- Facilita información sobre aquellos cambios informáticos y de comunicación previstos que puedan impactar en el SGCN y la documentación relativa a los riesgos, controles, medios y pruebas realizadas con el objetivo de que ésta pueda mantener dicho sistema documentado y adecuadamente coordinado e integrado.
- Dota a los sistemas de información de SCA, de los medios técnicos para que, en caso de sufrir alguna interrupción en sus sistemas y procedimientos, se preserven los datos y funciones esenciales y se mantengan las actividades de seguro y reaseguro o, de no ser posible, que tales datos y funciones se recuperen oportunamente y sus actividades de seguro o reaseguro se reanuden oportunamente, según los criterios definidos en el Análisis de Impacto corporativo.
- Opera un proceso de gestión y control de cambios en su infraestructura critica, (software, hardware, firmware, sistemas o aspectos y configuraciones de redes y comunicaciones, etc…), para asegurar que los cambios operados en dichas infraestructuras se registran, prueban, valoran, aprueban, implementan y verifican de una forma autorizada y controlada.

2.9. Dirección de Control de Riesgos

- Supervisará el alineamiento del SGCN con el Sistema de Gestión de Riesgos y el Sistema de Control Interno. Con una visión transversal a todos los riesgos de SCA, supervisará el marco general de gestión de los riesgos de resiliencia operativa y continuidad de negocio y apoyará las medidas oportunas para su desarrollo efectivo y adecuado seguimiento.
- De acuerdo con las responsabilidades atribuidas en la Política de Gestión del Riesgo Operacional, supervisará e informará al Comité de Continuidad y Resiliencia TI de los siguientes aspectos:
  - Resultados y conclusiones del proceso de identificación y autoevaluación de riesgos y controles y la valoración de riesgo inherente y residual de las categorías de riesgos relacionados con la resiliencia operativa y la continuidad de negocio.
  - Informará de los resultados alcanzados en la evaluación de escenarios de riesgo operacional en el ámbito de los riesgos relacionados con la resiliencia operativa y la continuidad de negocio, si procede.

2.10. Dirección de Comunicación

- Colabora con la Dirección de Seguridad Digital y Continuidad en la elaboración y la implementación de los aspectos del SGCN relacionados con la función de comunicación en casos de crisis o contingencias.
- Colabora con la Dirección de Seguridad Digital y Continuidad en la gestión de los canales de comunicación alternativos necesarios para que, en caso de sufrir alguna interrupción en sus sistemas y procedimientos, se reduzca el impacto en los clientes y reputacional, y se informe a las partes interesadas.
- Verifica y aprueba los planes de comunicación en caso de crisis, asegurándose de que están debidamente actualizados.
- Se asegura de implementar los canales de comunicación internos y externos necesarios para la notificación y la remisión de notas informativas en contingencia, así como de analizar, valorar, decidir y posteriormente dar a conocer, las directrices a través de las cuales se realizará la comunicación en caso de crisis.
- Define el mensaje, la estrategia y los medios y los canales de comunicación utilizados en caso de crisis y se encarga de nombrar un portavoz de la Compañía que, en caso de contingencia, se encargue de realizar las notificaciones a los medios de comunicación.
- Apoya a los gestores del SGCN en la realización de pruebas periódicas que afecten a su área de actividad.
- En el ámbito de la comunicación, dispone, actualiza y divulga un “Manual de gestión de crisis” que pone a disposición del SGCN para cuando sea de aplicación.

2.11. Unidades Operativas

- De acuerdo a los procedimientos, metodologías y con el soporte de la Dirección de Seguridad Digital y Continuidad, son las responsables de la identificación y evaluación de los riesgos de resiliencia operativa y continuidad de negocio, del establecimiento de los controles y las medidas oportunas para su mitigación, de colaborar en la documentación de los mismos así como de informar a la mayor brevedad posible a la Dirección Seguridad Digital y Continuidad de cualquier modificación en los procesos y medios que tengan previstos y de las incidencia que puedan afectar o afecten al normal desarrollo de sus actividades y siempre que estas impacten en el SGCN.
- Colaboran en los procesos de crisis de acuerdo a los planes y procesos establecidos y a las instrucciones que reciban de la Dirección de Seguridad Digital y Continuidad y/o del Comité de Continuidad de Negocio y Resiliencia TI.
- El resto de áreas y departamentos de SCA que puedan intervenir como actores o puedan verse afectados en caso de contingencias, tienen definidas sus actividades y obligaciones en el documento de definición de roles y responsabilidades del SGCN.

3. Estrategia, Procesos y Procedimientos

3.1. Estrategia

Ante la posibilidad de indisponibilidad de un Activo Crítico derivado de una contingencia, las estrategias diseñadas e implantadas en SCA para mitigar dicho impacto, son las de dotar a la compañía de activos críticos alternativos que suplen la indisponibilidad del anterior.

SCA ha definido cuatro Activos Críticos principales:

- Personas,
- Sedes,
- Proveedores,
- Conjunto de Datos y Sistemas que operan en la entidad.

Cada uno de ellos, dispone de una diferente estrategia de recuperación o de continuidad de negocio para hacer frente a sucesos disruptivos que los afecten y que se detallan a continuación:

- Activos Críticos Personas y Sedes: La estrategia para la gestión de contingencias que afecten a estos activos críticos, consiste, mediante criterios de coste-beneficio, en dotarse de personal alternativo adecuadamente formado, así como de sedes alternativas o de contingencia en las que poder desarrollar las tareas críticas en caso de que estos activos se vean afectados por un suceso disruptivo. En su defecto y para el caso de afectaciones a sedes, se prevé activar las estrategias de teletrabajo implantadas en SCA.
- Activo Crítico Proveedores: La estrategia para la gestión de contingencias que afecten a los proveedores que prestan servicios a la entidad, es la siguiente:
    - 1º Redundar aquellos proveedores que sea factible, siguiendo criterios apropiados de coste – beneficio.
    - 2º Internalizar la actividad de aquellos proveedores relevantes, que, por su menor tamaño, sea factible hacerlo con recursos de SCA en caso de contingencia.
    - 3º Controlar al resto de proveedores a los que no se les apliquen las estrategias anteriores y para ello, implantar y mantener una estrategia de control y verificación periódica, (anual), de sus capacidades de continuidad de negocio, validando y evidenciando que están dotados de un Sistema de Gestión de la Continuidad de Negocio, (SGCN), operativo, que idóneamente esté estandarizado, (ISO 22301), y que se revisan mediante la realización de auditorías y pruebas periódicas del mismo.
    - 4º Para aquellos proveedores de SCA clasificados como Críticos, titulares de prestación de servicios externalizados y en sintonía con lo expresado en la Política de Externalización de Servicios Críticos, se operará conjuntamente con la Dirección de Compras para lograr el cumplimiento coherente de lo expresado por ambas políticas.
- Activo Crítico Sistemas de Información: La estrategia diseñada en SCA, para la gestión de contingencias que afecten a este activo crítico, es la de mantener centros de procesos

de datos redundados e independientes, con las aplicaciones y sistemas críticos adecuadamente redundados y en una disposición operativa de seguridad y balanceo de carga, de forma que no haya un punto de fallo único que pueda afectar a la disponibilidad y operatividad de las aplicaciones críticas de la entidad.

- La gestión de este activo está desarrollada en el cuerpo normativo de Continuidad de negocio que recoge específicamente, aspectos de resiliencia TI.

  Adicionalmente se mantiene sobre dichos activos, un proceso de mejora continua, analizando nuevos escenarios que impliquen situaciones de indisponibilidad total en ambos centros y dotación de planes de contingencia.

  En el caso de que dichos activos estén externalizados en proveedores de servicios Cloud, la estrategia de continuidad, pasará por el diseño, la revisión e implantación de acuerdos de nivel de servicio, realización de pruebas, auditorias y revisiones de cumplimiento, que garanticen la disponibilidad de los mismos en los términos requeridos por la entidad, así como el cumplimiento de las normativas vigentes que les sean de aplicación.

3.2. Procesos

SCA ha desarrollado los procesos y procedimientos necesarios para llevar a cabo la función de continuidad de negocio y que se necesiten para cumplir con sus obligaciones en este ámbito.

3.2.1. Modelo de gestión de los riesgos de continuidad de negocio

El SGCN de SCA comprende en todo momento, un conjunto de elementos necesarios para garantizar la continuidad de las operaciones y servicios en caso de incidente y que es proporcional a la naturaleza, volumen y complejidad de sus operaciones.

Estos elementos o procesos básicos, del SGCN, son los siguientes:

1. Análisis de Impacto:

El análisis de Impacto, (en adelante BIA – de las siglas en inglés Business Impact Analysis): es el proceso que permite identificar el impacto en la Entidad, que causaría una interrupción de un proceso o actividad crítica (1), dependiendo de la duración y afectación de dicha interrupción.

De igual modo contemplará dos impactos adicionales: El fraude a través de la alteración de los datos en sistemas de la entidad (Integridad) y el acceso o exfiltración de información no autorizado (Confidencialidad).

Su revisión y actualización, se realizará periódicamente o ante cualquier cambio relevante, por el personal responsable de la Continuidad de Negocio, adscrito a la Dirección de Seguridad Digital y Continuidad.

[1] Se define como Actividad Crítica, aquella cuya interrupción genera impacto de nivel alto o muy alto en un plazo entre 24 y 48h. en cualquiera de las variables que se valoran para ello: operacional, legal, financiera o reputacional.

Permite, desde el punto de vista de continuidad, clasificar los procesos de SCA en diferentes categorías de criticidad, (muy alta o crítica, alta, media y baja), y definir tiempos objetivos de recuperación, (RTOs).

En función de dicha criticidad, sirve de base para la definición de requerimientos para el SGCN, los DRP, ("Disaster Recovery Plans") y los Planes de Comunicación de Crisis, que partirán de las especificaciones del BIA, para definir los tiempos y medios adecuados para la recuperación del sistema y asegurar los niveles de servicio definidos.

Tanto los resultados de los análisis de impacto, como la visión integral de los Análisis de Riesgos, se presentarán para su revisión y aprobación por el Comité de Continuidad de Negocio y Resiliencia TI.

En el análisis de impacto, se consideran los siguientes impactos:

- Escenario de pérdida de indisponibilidad (Continuidad)
  - Clientes
  - Legal/regulatorio
  - Financiero
  - Operativo
- Escenario de fraude (Integridad):
  - Clientes
  - Legal/regulatorio
  - Financiero
  - Operativo
- Clasificación de la Información (Confidencialidad):
  - Clasificación de la Información

La información que recoge este análisis de impacto, con indicación de las actividades que se consideran críticas en SCA, es la siguiente:

- Relación de unidades organizativas que realizan actividades críticas, sus funciones y los colaboradores necesarios para operarlas.

- Relación de instalaciones y sedes en las que se operan las indicadas actividades identificadas como críticas.

- Relación de aplicaciones soporte para la ejecución de las actividades críticas.

- Relación de proveedores que apoyan, suministran o intervienen en la ejecución de dichas tareas críticas.

- Intensidad del impacto para cada uno de los tipos o valores de impacto definidos y la evolución de estos en función de los diferentes plazos de recuperación de las actividades críticas que se hayan visto afectadas en una contingencia.

2. Análisis de riesgos de resiliencia operativa y continuidad de negocio:

El Análisis de Riesgos es el procedimiento que permite identificar y analizar los diferentes factores de riesgo que potencialmente puedan afectar a los activos que se quiere proteger.

El resultado de este análisis ayudará a definir los escenarios de desastre.

Estos análisis, se actualizarán periódicamente y, en cualquier caso, siempre que se produzcan cambios relevantes que puedan afectar, de forma significativa, a la situación, valoración o cuantía de los riesgos de continuidad de la entidad.

Mitigación y gestión de los riesgos de resiliencia operativa y continuidad de negocio:

Las áreas operativas y de soporte, establecerán los controles y las medidas oportunas para mitigar los riesgos de continuidad que se encuentren bajo su ámbito de responsabilidad, para mantener la valoración de los mismos en los niveles deseados y tomando en consideración la estrategia de riesgo aprobada por el Consejo de Administración.

Adicionalmente, se definirán y mantendrán planes de respuesta que deberían activarse ante la posible materialización de riesgos relacionados con la continuidad de negocio por fallos originados en los controles y medidas de mitigación de riesgos establecidas.

De forma alternativa a los planes de respuesta mencionados, se han diseñado y formalizado planes de contingencia operativos, (PCOs), para activar en el caso de que la operación de los planes de contingencia tecnológica no sea viable a corto plazo y en al caso de afecten a infraestructuras o servicios críticos, o en caso de que se produzcan contingencias en proveedores críticos de servicios TIC, en consonancia con las recomendaciones de la AESPJ.

En este último escenario, se han basará en el inventario de los proveedores de servicios críticos de infraestructura TIC y deberá poder mitigar contingencias en los mismos.

Planes de Recuperación, Equipos de Contingencia y Protocolos de Gestión y Comunicación:

SCA dispone de un conjunto flexible de procedimientos de respuesta pre-elaborados que permiten una reacción rápida y que regulan la recuperación de las actividades críticas, contemplando los escenarios de contingencia que puedan afectar a los diversos activos críticos de la entidad y para sus sedes principales, delegaciones y demás localizaciones en las que opera SCA y sus entidades afines.

Estos módulos de respuesta, se denominan Planes de Recuperación y cada infraestructura y Activo Crítico de SCA, tiene un Plan específico de Recuperación, un Equipo de Contingencia que se encarga de gestionarlo y por encima de él, un Equipo de Gestión de Incidentes, (en adelante EGI), que lo activa y supervisa su funcionamiento.

Para llevar a cabo estos Planes de Continuidad SCA ha:

- Definido y formado Equipos de Contingencia entrenados en la recuperación de los activos soporte de procesos de negocio críticos, con ámbitos de actuación claramente definidos y una cadena designada de comunicación y mando liderada por un Equipo de Gestión de Incidentes, (EGI), formalmente nominado.
- Definido e implantado protocolos de activación y gestión de incidentes.
- Establecido canales claros de comunicación soportados por planes de comunicación externos e internos.
- Establecido criterios claros que permitan determinar todos los hechos causantes de la crisis, que contengan directrices para la recopilación de información, así como para la realización de una investigación exhaustiva que determine los posibles hechos, responsabilidades y defensas disponibles.

- Diseñado e implantado procedimientos para generar informes sobre incidentes resueltos, conteniendo detalles de lo ocurrido, de las acciones llevadas a cabo, del cumplimiento de los objetivos del Plan de Continuidad, de los tiempos empleados y de las dificultades encontradas. Dichos informes deben valorar si el Plan ha funcionado según lo planeado y establecer en su caso, las acciones de mejora correspondientes.

3. Programas de concienciación y formación:

SCA dispone de un programa para la difusión de información en materia de continuidad de negocio y resiliencia TI, que permite construir una cultura de continuidad en todos los niveles de la organización.

Dispone también, de un programa detallado y específico de formación para garantizar que los equipos designados para la gestión de contingencias y especializados en la resolución de incidentes de continuidad, desarrollen y se actualicen en las competencias suficientes para que añadan el valor necesario tanto en el mantenimiento del sistema, como durante los procesos de recuperación ante la ocurrencia de incidentes.

Ambos programas están documentados y su operación y gestión está a cargo del personal de Continuidad de Negocio y Resiliencia TI adscrito a la Dirección de Seguridad Digital y Continuidad.

En lo referente a Resiliencia TI, la función, desarrollará, implantará e impartirá los programas de concienciación y formación técnicos y operativos que, por la especificidad de sus recursos y activos, se hayan de acometer; alineados con el modelo de Continuidad de Negocio.

4. Sistemática de mejora continua:

SCA dispone de una sistemática de gestión para la mejora continua que incluye indicadores del estado y capacidades del SGCN, así como los niveles objetivos definidos para alcanzar a lo largo del tiempo, recogidos en un cuadro de mando para su seguimiento anual, que permite la elaboración de informes de gestión.

La ejecución de esta sistemática, está a cargo del personal de Continuidad de Negocio adscrito a la Dirección de Seguridad Digital y Continuidad.

3.2.2. Verificación del funcionamiento del Sistema

Se realizarán las siguientes actividades encaminadas a verificar el correcto funcionamiento y la mejora continua del SGCN:

1. **Escenarios de desastre:**

La entidad dispone de un juego representativo de escenarios posibles que sirvan para orientar el plan y priorizar los esfuerzos y que, en particular, se concretan en planes de recuperación para los siguientes escenarios de desastre que se detallan a continuación.

- Escenarios de indisponibilidad del Activo Crítico Sedes;
  - Indisponibilidad de Sedes y Servicios Centrales.
  - Indisponibilidad de grandes Delegaciones.
  - Indisponibilidad de pequeñas y medianas Delegaciones.

- Escenarios que afecten al Activo Critico Personas:
  - Indisponibilidad de personal crítico.
- Escenarios que afecten al Activo Crítico Proveedores:
  - Indisponibilidad de Proveedores Críticos.
  - Indisponibilidad de Proveedores Relevantes.
- Escenarios que afecten al Activo Crítico Sistemas:
  - Pérdida del Data Center M1.
  - Pérdida del Data Center M2.
  - Pérdida de Almacenamiento Centralizado, (M1 o M2).
  - Pérdida de la red LAN del Data Center. (M1 o M2).
  - Indisponibilidad total de sistemas, (Escenario de Afectación Total o Ciberataque).

El tipo de suceso, el grado de afectación a los activos críticos de la entidad, (Conjunto de Personas, Proveedores, Datos y Sistemas y Sedes afectados), conforma los que se denominan “Escenarios de Continuidad” o “Escenarios de Desastre”.

Los mismos, estarán sujetos a revisión y pruebas periódicas, auditoria, estandarización y a los procesos de mejora que se indican en los apartados siguientes.

2. **Plan de pruebas y mantenimiento:**

La Dirección de Seguridad Digital y Continuidad coordina un programa de pruebas y ejercicios anuales de simulación que permiten verificar que los Planes de Recuperación obtienen los resultados previstos en el plazo acordado, recogiendo de forma estructurada y detallada todas las desviaciones detectadas para corregirlas.

Dichos planes, cumplen con los requisitos regulatorios indicados por la legislación aplicable y detallada en el Anexo de esta Política, están documentados y su gestión está a cargo del personal de Continuidad de Negocio y Resiliencia TI adscrito a la Dirección de Seguridad Digital y Continuidad.

El alcance de las pruebas a realizar, deberá definirse y ser aprobado por el Comité de Continuidad de Negocio y Resiliencia TI.

La Dirección de Seguridad Digital y Continuidad emite un informe anual revisado y aprobado en el Comité de Continuidad de Negocio y Resiliencia TI sobre la situación del SGCN y que incorpora como mínimo:

- Los resultados de las pruebas planificadas durante el año.
- El resumen de los incidentes más relevantes ocurridos durante el ejercicio.
- Propuestas de mejora ejecutadas en el ejercicio.
- Situación de los planes de acción para las mejoras identificadas.

- Evolución de los riesgos e impactos.

Los resultados de las pruebas realizadas, sus informes y planes de mejora y calendarios de implementación, se pondrán a disposición del comité de continuidad y se remitirán a terceras partes interesadas, bajo solicitud y en particular, al regulador.

Así mismo, dichos resultados, y lecciones aprendidas, se incorporarán a los procedimientos de testeo siguiendo un proceso de mejora continua.

3.2.3. Procedimientos

A continuación se detallan los procedimientos específicos de continuidad:

- Instrucciones para la elaboración de los BIAS y el Análisis de Riesgos.
- Instrucciones para la ejecución de Pruebas.
- Plan de Gestión de Incidentes.
- Planes de Comunicación Interna y Externa o de Gestión de Crisis.
- Planes de Recuperación.
- Instrucciones de Recolocación del Personal.
- Planes de Emergencia y Evacuación.
- Manual de Gestión de Crisis.
- DRPs de las aplicaciones y servicios tecnológicos críticos.
- Plan de Pruebas de TI.
- Plan de Formación en Contingencia TI.
- Plan de Contingencia TI.

Adicionalmente existen otros documentos que aplican a Continuidad como parte del área de Seguridad, relacionados con las certificaciones ISO 22301 e ISO 27001.

4. Reporting

4.1. Reporting interno

4.1.1. Reporting al Comité de Continuidad de Negocio y Resiliencia TI

Todo el conjunto de tareas ejecutadas para la gestión y soporte del SGCN de SCA, operadas por el personal de Continuidad de Negocio y Resiliencia TI, serán reportadas semestralmente o ante evento relevante por parte de la Dirección de Seguridad Digital y Continuidad en Comité de Continuidad de Negocio y Resiliencia TI.

De acuerdo con las atribuciones establecidas en esta política se le informará de los siguientes aspectos:

1. Presupuestos del SGCN, así como de los recursos humanos, técnicos y económicos disponibles para garantizar su correcto funcionamiento.
2. Planes de Formación y Concienciación en el ámbito del SGCN y de los riesgos de resiliencia operativa y continuidad de negocio.
3. Manuales y procedimientos definidos en el SGCN.
4. Análisis de impacto (BIAs), así como de los riesgos de resiliencia operativa y continuidad de negocio.
5. Planes de Continuidad y Resiliencia TI, así como del estado de las iniciativas en este último ámbito.
6. Planes de Recuperación de Desastre o “Disaster Recovery Plans”, (DRPs).
7. Seguimiento de los indicadores de riesgo y métricas de desempeño de Continuidad de negocio y Resiliencia TI.
8. Resultados del proceso de autoevaluación de riesgos y controles y de los resultados alcanzados en la evaluación de escenarios de riesgo operacional relacionados con la resiliencia operativa y la continuidad de negocio.
9. Los resultados de las pruebas realizadas sobre los Planes de Continuidad de Negocio y de las deficiencias identificadas.

Igualmente, se presentará para su validación el Informe Anual de Continuidad de Negocio y Resiliencia TI que deberá contener los hechos más relevantes de los aspectos anteriormente mencionados.

4.1.2. Reporting al Comité de Dirección.

A efectos de supervisión, se le reportará el Informe Anual de Continuidad de Negocio y Resiliencia TI.

Dicho informe anual, se generará y reportará cerrado el ejercicio.

Igualmente, se le informará de los resultados de las pruebas realizadas sobre los Planes de Continuidad de Negocio y las deficiencias identificadas, así como de los incidentes de

continuidad sobre cualquier activo crítico que se consideren relevantes por parte del Comité de Continuidad de Negocio y Resiliencia TI.

4.1.3. Reporting al Comité de Riesgos

Se le informará sobre el Informe Anual de Continuidad de Negocio y Resiliencia TI y en particular se le informará sobre los siguientes aspectos:

1. Análisis de impacto (BIAs), así como de los riesgos de resiliencia operativa y continuidad de negocio.
2. Resultados de los Planes de Recuperación de Desastre o “Disaster Recovery Plans”, (DRPs).
3. Seguimiento de los indicadores de riesgo y métricas de desempeño de Continuidad de negocio y Resiliencia TI.
4. Resultados del proceso de autoevaluación de riesgos y controles relacionados con la resiliencia operativa y la continuidad de negocio, así como de los resultados alcanzados en la evaluación de escenarios de riesgo operacional.

Igualmente, se le informará de los resultados de las pruebas realizadas sobre los Planes de Continuidad de Negocio y las deficiencias identificadas, así como de los incidentes de continuidad sobre cualquier activo crítico que se consideren relevantes por parte del Comité de Continuidad de Negocio y Resiliencia TI.

4.1.4. Reporting a la Comisión de Auditoría

Se le informará sobre todos los aspectos relevantes del Informe Anual de Continuidad de Negocio y Resiliencia TI, informando en particular sobre los riesgos de resiliencia operativa y continuidad de negocio.

Igualmente, se le informará sobre los resultados de las pruebas realizadas sobre los Planes de Continuidad de Negocio y de las deficiencias identificadas, así como de los incidentes de continuidad que hayan afectado de forma relevante a cualquier activo crítico y que se consideren significativos.

4.1.5. Reporting al Consejo de Administración

Será informado de los incidentes o hechos relevantes que afecten severamente a la Continuidad de Negocio, de las deficiencias identificadas como resultado de las pruebas realizadas sobre los planes de continuidad de negocio, así como de cualquier otro aspecto que requiera el Consejo de Administración.

4.2. Reporte a los organismos supervisores

SCA informará al supervisor sobre cualquier aspecto relativo al SGCN cuando sea requerido por cualquier circunstancia.

Anexo: Referencias normativas

La normativa que ha servido de base para el desarrollo de esta Política, queda especificada en la Política marco de Gestión de Riesgos.

De forma adicional, existen diversas normativas de distintos ámbitos reguladores que establecen aspectos relevantes que son de aplicación, y que igualmente se han utilizado para la elaboración de la presente Política:

- Directrices EIOPA sobre gobernanza y seguridad de las tecnologías de la información y de las comunicaciones (EIOPA – BoS – 20/600, ES).
- Reglamento General de Protección de Datos, (RGPD), Reglamento relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- ISO/IEC 22301 “Security and Resilience — Business Continuity Management Systems” — Requirements”.
- Directrices (BoS-20/002) de EIOPA sobre externalización a proveedores de servicios en la nube.
- Guía Técnica 2/2017 de la Dirección General de Seguros y Fondos de Pensiones sobre cuestiones en materia de Sistema de Gobierno.
- ISO/IEC 27001 "Information technology - Security techniques - Information security management systems - Requirements".
- ISO/IEC 27002 "Information technology - Security techniques - Code of practice for information security controls".
- ISO/IEC 27005 "Information technology - Security techniques - Risk Management of Information Security".
- ISO/IEC 27017 “Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services”.
- Reglamento de Resiliencia Operativa Digital (DORA), proyecto del reglamento del parlamento europeo y del consejo sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology.
- Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE).

Fin de documento: PL01208 Política de Continuidad de Negocio.docx