POLÍTICA DE CONTINUIDAD DE NEGOCIO
RESUMEN WEB

Índice

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

Política de Continuidad de Negocio

Fecha de aprobación:	16 de Diciembre de 2021
Responsable de edición y revisión	D.A. 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

1. Introducción

La presente Política se enmarca en el Sistema de Gobierno y de gestión de riesgos establecido por SegurCaixa Adeslas.

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.

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.

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.

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, 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. Estrategia, Procesos y Procedimientos

2.1. 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 Área de Compras y G. Externalización 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.

  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.

2.2. 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.

2.2.1. 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.

Su revisión y actualización, se ejecuta con periodicidad anual o ante cualquier cambio relevante, por el personal responsable de la Continuidad de Negocio, adscrito a la Dirección de Área de Seguridad Digital y Continuidad.

En el análisis de impacto, se consideran cuatro tipos de variables:

- Operacional,
- Legal,
- Financiero y
- Reputacional.

2. Análisis de Riesgos 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.

Estos análisis, se actualizan como mínimo anualmente 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.

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.

[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.

- 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.

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.

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 Área de Seguridad Digital y Continuidad.

2.2.2. 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.

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”.

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

SCA ejecuta 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 Área de Seguridad Digital y Continuidad.

El alcance de las pruebas a realizar, deberá comprender la totalidad de activos críticos de la entidad.

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.

2.2.3. Procedimientos

Todos estos procesos y sus elementos, están desarrollados de una manera más detallada en sus respectivos Manuales y Procedimientos de Continuidad de Negocio; que se concretan en el siguiente conjunto de documentos:

- Documentos de Gestión.
- Instrucciones Técnicas.
- Planes de Respuesta.
- Cuerpo documental de Contingencia TI.

Todo este conjunto documental, está gestionado por las unidades indicadas anteriormente en la Política y está soportado en una herramienta de un tercero.

SCA, está dando los pasos necesarios para implementar y mantener la estandarización del mismo bajo el estándar ISO 22301 mencionado en el anexo de esta política.

3. Reporting

3.1. Reporting interno

3.1.1. 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 Área de Seguridad Digital y Continuidad en Comité de Continuidad de Negocio y Resiliencia TI.

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.

3.1.2. Reporting al Comité de Dirección.

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

3.1.3. Reporting al Comité de Riesgos

Se le informará sobre el Informe Anual de Continuidad de Negocio y Resiliencia TI.

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.

3.1.4. 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.

3.1.5. 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.

3.2. 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 22301:2019 “Security and Resilience — Business Continuity Management Systems” — Requirements”.

Fin de documento: PL012.05 Política de Continuidad de Negocio.docx