POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Índice

La presente política ha sido analizada por el Comité de Dirección y el Comité de Riesgos, proponiendo el visto bueno de la Comisión de Auditoría y la aprobación del 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 seguridad de la Información

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	14/12/2023	Edición	D.A Seguridad Digital y Continuidad	Consejo de Administración
02	14/12/2024	Modificación	D.Seguridad Digital y Continuidad	Consejo de Administración

La presente política ha sido realizada por:

- Dirección de Seguridad Digital y Continuidad: ha garantizado 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.
- Dirección de Control de Riesgos: ha supervisado la coherencia de esta Política con el resto de las 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 de seguridad.

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 marco normativo emanado de las Directrices sobre Gobernanza y Seguridad de las Tecnologías de la Información y de las Comunicaciones emitidas por la EIOPA, así como en el *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) han puesto de manifiesto la necesidad de contar con una política de Seguridad que establezca las bases para la gestión de sus medidas de seguridad. Adicionalmente, cada vez más, los procesos de las entidades aseguradoras y bancarias se apalancan en la digitalización, el empleo de nuevas tecnologías y en la contratación de proveedores. La tendencia al alza de dicha digitalización deriva en un aumento en los riesgos de seguridad de sus activos de información que obliga a que su dirección, a través del órgano competente, defina los principios a alto nivel y las normas destinadas a proteger la confidencialidad, la integridad y la disponibilidad de la información a fin de respaldar la aplicación de la estrategia de sus tecnologías de información.

En este sentido, SegurCaixa Adeslas ha procedido a la redacción de una política de seguridad de la información.

La normativa general que ha servido de base para el desarrollo de esta política queda especificada en la Política marco de Gestión de Riesgos y en las políticas de Riesgo Operacional y Control Interno. De forma adicional, existen otras normas, directrices y prácticas de mercado que establecen requerimientos y recomendaciones para la seguridad de la información. Esta normativa es recogida en el Anexo I de la presente Política.

1.2. Compromiso del Órgano de Administración

El Consejo de Administración de SegurCaixa Adeslas, dentro de la estrategia global definida para el desarrollo del negocio, considera la gestión de la Seguridad de la Información y de los datos personales como un aspecto vital para garantizar la consecución de los objetivos de negocio definidos.

El Consejo de Administración se compromete a fomentar que se gestionen adecuadamente los objetivos de Seguridad de la Información y se lleve a cabo, por tanto, una correcta gestión de riesgos y control interno derivados tanto de los mismos, como de los recursos necesarios para el cumplimiento de la presente Política.

1.3. Objetivos de la política

El objetivo de la presente política es establecer el marco general que es necesario, con sus principios y características generales, para garantizar una gestión eficaz de la seguridad de las tecnologías de la información y de las comunicaciones (en adelante también “TIC”), así como de proporcionar el marco para el establecimiento de los objetivos de seguridad de la información de la Compañía.

En este sentido, la presente Política vela por la Seguridad de la Información en todos los procesos de negocio de SegurCaixa Adeslas mediante el control y gestión del riesgo tecnológico. Define los requisitos mínimos de Seguridad dentro de ésta, a través del establecimiento de una estrategia basada en un modelo de mejora continua para la prevención, detección y reacción ante cualquiera de las amenazas o riesgos que afecten a la Seguridad de la Información de SegurCaixa Adeslas en el desarrollo de sus servicios y actividades, así como reducir el riesgo introducido por el uso de las tecnologías de información en los procesos y servicios de la Compañía.

Con el fin de asegurar que la gestión de la Seguridad se alinea en todo momento con las necesidades de la organización, se establece una metodología de no conformidades, recomendaciones y mejora continua de todo el sistema de gobierno, siguiendo un ciclo “Plan-Do-Check-Act” (PDCA), que garantiza el mantenimiento continuo de los niveles de seguridad deseados.

Por tanto, la presente política supone el compromiso por parte del órgano de administración de:

- Establecer, implementar, operar, monitorizar, revisar y mejorar la gestión de la seguridad basada en la normativa estándar UNE-ISO/IEC 27001 (en adelante ISO 27001).
- Asignar las personas y recursos materiales adecuados para gestionar la seguridad.
- La Gestión de la Seguridad se adaptará a las necesidades de las partes interesadas
- Delegar funciones (salvo las aprobaciones propias de sus competencias) en los integrantes del Comité de Seguridad de la Información.
- Contribuir a la eficacia del sistema de gestión de seguridad.

1.4. Principios generales de la seguridad de la información

Mediante la presente política, se declaran como principios generales de la seguridad de la información los siguientes:

- Garantizar la confidencialidad, integridad y disponibilidad de toda la información procesada o albergada en el ámbito de la compañía.
- Asegurar todos los activos bajo su responsabilidad mediante las medidas que sean necesarias.
- Garantizar la continuidad de los servicios TI.

- Minimizar el impacto que cualquier tipo de incidente producido sobre la tecnología o la seguridad de la información pueda producir, independientemente de su origen y características.
- Asegurar que el apetito de riesgo de la entidad en el marco de los riesgos tecnológicos y de seguridad de la información, está establecido y se mantiene en los niveles pertinentes dentro de la organización.
- Satisfacer y cumplir los aspectos relativos a lo dispuesto en leyes y regulaciones, así como en los estándares voluntariamente asumidos.
- Llevar a cabo las sesiones de concienciación y formación específicas que permitan a cada uno de los diferentes perfiles conocer sus funciones en materia de Seguridad.
- Establecer los mecanismos oportunos que permitan la mejora continua.
- Establecer canales de comunicación e información adecuados para permitir el cumplimiento de sus obligaciones a nivel de Grupo.

De cara a establecer las herramientas para la consecución de dichos principios, las áreas responsables podrán establecer normativa interna más específica sobre la seguridad de la información. De la misma forma, también establecerán y aplicarán procedimientos y medidas más específicas para, entre otras cosas, mitigar los riesgos de TIC y seguridad a los que estén expuestas.

Todo ello da respuesta a EIOPA en su directriz 6 (Política y medidas de seguridad de la información) por la cual se exige a las empresas que instauren una política escrita de seguridad de la información aprobada por el OADS en la que se deberán definir los principios de alto nivel y las normas para proteger la confidencialidad, la integridad y la disponibilidad de la información de las empresas a fin de respaldar la aplicación de la estrategia de TIC y a lo previsto en el artículo 9.4 de DORA que requiere elaborar y documentar una política de seguridad de la información que defina normas para proteger la confidencialidad, disponibilidad, integridad o autenticidad de los datos, activos de información y activos de TIC, incluidos los de sus clientes.

1.5. Alcance

Este documento aplica a SegurCaixa Adeslas como entidad individual y a sus empleados, así como a los proveedores que le prestan servicios a SegurCaixa Adeslas, en la medida que sean de aplicación las obligaciones que se derivan de esta política.

2. Gobernanza, Funciones y Responsabilidades

Con objeto de garantizar el cumplimiento y evolución de los principios de la Gestión de la Seguridad de la Información, así como reportar y comunicar periódicamente el estado de la misma en SegurCaixa Adeslas, se definen las siguientes obligaciones y responsabilidades.

2.1. Consejo de Administración

En relación con lo expuesto en la Política de Gestión y Control del Riesgo Tecnológico respecto a las funciones del Consejo, en lo que concierne a la Seguridad de la Información, estas son sus atribuciones:

- Asumirá la responsabilidad última de gestionar el riesgo relacionado con las TIC.
- Aprobar, supervisar y revisar la presente política.
- Establecer un modelo efectivo para gestionar la Seguridad de la Información dotándolo de recursos humanos, conocimientos y capacidades adecuados para la aplicación de la estrategia de seguridad.
- Asignará y revisará periódicamente el presupuesto adecuado para satisfacer las necesidades de resiliencia operativa digital de la entidad financiera con respecto a todos los tipos de recursos, incluidos los programas de sensibilización en materia de seguridad de las TIC y las actividades de formación sobre resiliencia operativa digital pertinentes.
- Aprobar, supervisar y revisar el Informe sobre la revisión del Marco de Control de Riesgos TI.
- Establecer canales de comunicación para mantenerse informado de los incidentes graves relacionados con las TIC y sus repercusiones, así como de las medidas de respuesta, recuperación y corrección.
- Establecer y aprobar la estrategia de seguridad, incluida en el plan director de seguridad, en el marco de su estrategia empresarial general y en consonancia con esta y supervisará su comunicación y aplicación y velará por que el sistema de gobernanza, en especial el Sistema de Gestión de la Seguridad de la Información, se gestione adecuadamente.
- Tomar razón del asesoramiento por parte de la Dirección de Seguridad Digital y Continuidad, en la implantación y cumplimiento de la presente Política y de la normativa interna que la desarrolle, así como aprobar los resultados de los procesos de gestión de la Seguridad de la Información y su evolución, velando por que estos sean incluidos en el proceso de gestión de la seguridad de la empresa. Adoptar las decisiones que puedan corresponder.
- Promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la autenticidad, integridad, disponibilidad y confidencialidad de la información.
- Adoptar las actuaciones pertinentes ante incidentes en el ámbito de la seguridad de la información.

2.2. Comisión de Auditoría

- Supervisar la eficacia del control interno, la auditoría interna y el Sistema de Gestión de la Seguridad de la Información de la entidad, así como discutir con el auditor de cuentas las debilidades significativas del sistema de control interno detectadas en el desarrollo de la auditoría, todo ello sin quebrantar su independencia. A tales efectos, y cuando lo considere necesario, podrá presentar recomendaciones o propuestas al Consejo de Administración.
- Supervisar, antes de su presentación al Consejo de Administración, de los siguientes elementos:
    - La política de Seguridad de la Información.
    - La estrategia de Resiliencia Operativa Digital.
    - El presupuesto asociado a la Estrategia de Resiliencia Operativa Digital.
    - El informe sobre la revisión del Marco de Control de Riesgos TI.
    - El reporting sobre los resultados de los procesos de gestión de los riesgos tecnológicos y de Seguridad de la Información y su evolución.
    - El plan de auditorías TIC.

2.3. Comité de Riesgos

En el ámbito de la seguridad de la información se le atribuyen a este Comité, cuya composición se encuentra definida en la Política de Gestión de Riesgos, las siguientes competencias:

- Tomar conocimiento de la planificación anual de la Dirección de Seguridad Digital y Continuidad y de su ejecución.
- Revisar el modelo de gestión y control interno de seguridad de la información antes de su evaluación al Consejo de Administración.
- Como paso previo a su elevación a la Comisión de Auditoría y Consejo de Administración, supervisará:
    - Los informes sobre riesgos de seguridad elaborados y presentados por parte de la Dirección de Seguridad Digital y Continuidad como consecuencia de las competencias que se definen en esta Política.
    - La política de Seguridad de la Información.
    - La estrategia de Resiliencia Operativa Digital.
    - El informe sobre la revisión del Marco de Control de Riesgos TI.
- Estará involucrado en el proceso de gestión la seguridad de la información mediante la revisión de los resultados alcanzados, así como las recomendaciones y planes de acción que se establezcan, estando informado de los asuntos tratados y ocupándose de aquellos aspectos que se escalen por parte de los Comités de Seguridad Digital y de Continuidad de Negocio y Resiliencia TI.

2.4. Comité de Dirección

El Comité de Dirección, presidido por el Director General, es responsable de implantar dentro de la organización las medidas técnicas, organizativas y de control que garanticen la autenticidad, integridad, disponibilidad y confidencialidad de la información y de la implementación de una cultura de seguridad de la información. Las responsabilidades se concretan en las siguientes tareas:

- Es responsable de la implantación de un modelo de Gestión de la Seguridad de la Información, alineado con el Sistema de Gestión de Riesgos, bajo los criterios y parámetros establecidos por el Consejo de Administración. Para ello, encomendará a la Dirección de Tecnología y Transformación Tecnológica para que a través de la Dirección de Seguridad Digital y Continuidad desarrolle las acciones que sean necesarias para alcanzar tal fin trasladándole cualquier hecho o circunstancia relevante en el ámbito de la seguridad de la información.

- Definir la propuesta de estrategia de Seguridad de la Información, incluida en el Plan Director de Seguridad, antes de su elevación al Consejo de Administración.

- Deberá estar permanentemente involucrado en los procesos de la Seguridad de la Información y en la elaboración de informes y propuestas por parte del CISO a los órganos de gobierno, garantizando que la estrategia de seguridad se aplica, adopta y comunica a todo el personal y los proveedores de servicios pertinentes, según sea aplicable y relevante, de manera oportuna.

- Colaborar con la implementación del Cuerpo Normativo de Seguridad de la Información y la implantación de la estructura organizativa que permita su correcto seguimiento y cumplimiento.

2.5. Comité de Transformación Tecnológica

Las competencias y responsabilidades del Comité de Trasnformación Tecnológica, quedan recogidas en la política de gestión y Control del Riesgo Tecnológico.

2.6. Comité de Seguridad Digital

Son miembros permanentes de este Comité, al que informa el titular del área de Seguridad Digital:

- 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.

- El Delegado de Protección de Datos Personales.

- El Director de Desarrollo Corporativo.

- El Director de Organización y RRHH.

- El Director de Control de Riesgos.

- El Responsable de Continuidad y Resiliencia TI.

- El Responsable de Gobierno, Riesgo y Cumplimiento de Seguridad Digital, que actuará como Secretario del Comité.
- Adicionalmente podrán ser invitadas por el Comité otras áreas de negocio o personas que, por su conocimiento de las materias que se fueran a tratar en el orden del día, se considere oportuno.

En relación con la Seguridad de la Información se le atribuyen a este Comité, las siguientes competencias:

- Asegurar el Cumplimiento de la Estrategia TIC, la Política de Gestión y Control del Riesgo Tecnológico y Seguridad de la Información, y el alineamiento de las prioridades acordadas por los órganos de gobierno.
- Aprobar las propuestas de nuevos documentos del Cuerpo Normativo de Seguridad y revisiones/modificaciones sobre las existentes.
- Impulsar las acciones de robustecimiento y los planes de robustecimiento de Riesgos tecnológicos y Seguridad de la Información (Planes de Acción Rápida, Planes Directores de Seguridad, etc.).
- Hacer un seguimiento de los proyectos en curso y monitorización del avance.
- Solucionar bloqueos e impedimentos que impidan alcanzar los objetivos definidos de Seguridad de la Información, desde el punto de vista de confidencialidad e integridad.
- Elevar y aprobar decisiones estratégicas para con la Seguridad de la Información.
- Monitorizar la operativa de la Dirección de Seguridad Digital y Continuidad y asignación de recursos necesarios a través de la definición específica de Planes de Capacidad.
- Validar las definiciones y toma de requerimientos para la ejecución de iniciativas de Seguridad de la Información.
- Alinear y posteriormente proponer a los órganos de gobierno para su aprobación final por el Consejo de Administración de las iniciativas que deberán componer la estrategia de riesgos TIC y los niveles de apetito por el riesgo.
- Realizar el seguimiento de KPI’s de seguridad a nivel tanto operativo como estratégico.
- Comunicar y reportar Alertas, Amenazas, Riesgos e Incidentes de Seguridad relevantes. En aquellas circunstancias con repercusión en la continuidad de las actividades de SCA, decidirá sobre su escalado al Comité de Continuidad de Negocio y Resiliencia TI en los términos establecidos en la Política de Continuidad de Negocio.
- Decidir en el escalado de decisiones o cuestiones a ser revisadas por el Comité de Dirección y Comité de Riesgos de SCA.
- Realizar la propuesta de los niveles de apetito al riesgo de los riesgos TIC y evaluar su cumplimiento conforme a lo establecido en la Política de Gestión de Riesgos.
- Revisar, previo a su entrada en el circuito habitual de envíos de información al supervisor, de los siguientes elementos:

- Envío al menos una vez al año a las autoridades competentes información sobre el número de nuevos acuerdos relativos al uso de servicios de TIC, las categorías de proveedores terceros de servicios de TIC, el tipo de acuerdos contractuales y los servicios y funciones prestados en materia de TIC.
- Información a la autoridad competente cuando se proponga celebrar cualquier acuerdo contractual para el uso de servicios de TIC que sustenten funciones esenciales o importantes y cuando una función se haya convertido en esencial o importante.
- Envío de último informe aprobado por el Consejo de Administración sobre la revisión del Marco de Control de Riesgos TI al supervisor.

El CISO informará al Comité de Dirección y al Comité de Riesgos sobre los asuntos tratados en el Comité y elevará aquellos aspectos que se hayan escalado.

2.7. Dirección de Seguridad Digital y Continuidad

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. Del mismo modo, los cometidos del titular del departamento, como función de seguridad de la información y conforme a la directriz 7 de EIOPA, serán los que a continuación se relacionan:

- Apoyar al Consejo de Administración a definir y mantener la Política de Seguridad de la Información y controlar su implantación y difusión.
- Informar y aconsejar al Consejo de Administración periódicamente y en momentos puntuales sobre los resultados de los procesos de gestión de los riesgos tecnológicos y de Seguridad de la Información y su evolución.
- Supervisar y revisar la aplicación de las medidas de Seguridad de la Información.
- Asegurarse de que al utilizar proveedores de servicios se cumplen los requisitos en el ámbito de riesgos tecnológicos y de seguridad de la información.
- Asegurarse de que todos los empleados y proveedores de servicios que acceden a la información y los sistemas son adecuadamente informados de los requisitos de seguridad, por ejemplo, mediante sesiones de formación y sensibilización al respecto.
- Coordinar el análisis de los incidentes operativos o de seguridad y comunicar a los órganos de gobierno. Coordinar con la Dirección de Control de Riesgos la captura de aquellos incidentes con efecto económico que deban tener reflejo en la base de datos de eventos de pérdida de riesgo operacional tal y como establece la Política de gestión del riesgo operacional.

Así mismo, le corresponden al CISO (Chief Information Security Officer), Director de la Seguridad de la Información o Responsable de Seguridad de SegurCaixa Adeslas, las siguientes responsabilidades específicas:

- Alinear la estrategia de ciberseguridad con los objetivos de la empresa.
- Definir la normativa de Seguridad de la Información.
- Prevenir, detectar y analizar vulnerabilidades.

- Informar y reportar a dirección cualquier cuestión relacionada con la ciberseguridad.
- Dar respuesta rápida ante cualquier incidente de ciberseguridad.
- Instaurar programas de formación sobre seguridad de la información para todo el personal y programas periódicos de sensibilización sobre seguridad de la información.
- Establecer e implementar el "Cuerpo Normativo de Riesgos Tecnológicos y de Seguridad de la información".
- Garantizar la seguridad y privacidad de los datos de la empresa.
- Llevar a cabo el descubrimiento electrónico y las investigaciones forenses digitales.
- Identificar las necesidades del negocio en materia de seguridad.
- Trasladar la necesidad del negocio en materia de seguridad hacia tecnología.
- Establecer criterios mínimos de seguridad, de forma uniforme a toda la organización.
- Revisar que las implantaciones están acordes con los criterios mínimos de seguridad.
- Velar por el cumplimiento de las Políticas de Seguridad de la Información.
- Identificar y tratar los GAPs de la Seguridad de la Información.
- Gestión de la Resiliencia TI.
- Gestión de Riesgos TIC en la primera línea.

2.8. Dirección de Auditoría Interna

La gobernanza, los sistemas y los procesos de las empresas para sus riesgos de seguridad de la información deberán ser auditados de manera periódica y en consonancia con su correspondiente plan de auditoría por unos auditores dotados de unos conocimientos, unas competencias y una experiencia suficiente en seguridad de la información, a fin de garantizar de manera independiente su eficacia al Consejo de Administración.

La frecuencia y el objeto de estas auditorías deberán ser adecuados a los riesgos de seguridad pertinentes.

2.9. Obligaciones de los usuarios (resto de la organización)

Adicionalmente, todo el personal de SegurCaixa Adeslas debe:

- Informar a las funciones fundamentales y a la Dirección de Seguridad Digital y Continuidad de la información, de cualquier hecho relevante presente, o futuro y previsible, que pudiera afectar de forma significativa a la seguridad de la información, siempre bajo el marco de cumplimiento del Código de Conducta Telemática Empleados y resto de normativa interna de aplicación.
- Cumplir con la presente política, así como con todos los procedimientos asociados a ésta.

3. Estrategia, procesos y procedimientos

3.1. Criterios de Seguridad

La presente Política establece las directrices y líneas de actuación en materia de Seguridad de la Información que rigen el modo en que SCA gestiona y protege sus activos de información mediante la mitigación del riesgo.

Este marco de Criterios de Seguridad de la Información presenta los objetivos de Seguridad de la Información, incluido en el Plan Director de Seguridad, alineados con la Estrategia de Resiliencia Operativa Digital y el Plan Director de Seguridad de la Compañía, tales como la mitigación de los riesgos tecnológicos, la minimización de los impactos en caso de incidente de seguridad, o la garantía de que, en caso de emergencia de continuidad, el servicio proporcionado se garantizará siempre en las mismas condiciones de seguridad que los servicios prestados en condiciones normales.

Por norma general, el riesgo de seguridad podrá aceptarse, mitigarse, transferirse o evitarse, definiéndose el criterio umbral del riesgo de seguridad de forma alineada con la Dirección de Control de Riesgos, así como otros parámetros como el apetito o la concurrencia.

A continuación, se establecen los criterios de Seguridad de la Información que deben soportar los procesos de negocio de la compañía y protegen la confidencialidad, integridad y disponibilidad de los activos de información:

- La información de la que la Compañía es propietaria y/o depositario debe ser únicamente accesible para las personas debidamente autorizadas, pertenezcan o no a la Compañía.
- La presente Política de Seguridad, así como el resto del Cuerpo Normativo de Seguridad, debe ser accesible para todos los miembros de la Compañía. El Cuerpo Normativo de Seguridad se estructurará a partir de la presente Política, a través de Normas de Seguridad y Procedimientos de Seguridad, formando éstos parte de la Política.
- La Compañía debe cumplir con todos aquellos requerimientos legales, regulatorios y estatuarios que le sean de aplicación, así como los requerimientos contractuales que afecten a la Seguridad de la Información.
- La Compañía deberá establecer medidas de supervisión y monitorización continuas de los riesgos TIC, abarcando al menos: factores internos y externos, proveedores y otras entidades y amenazas internas y externas.
- La aplicación de los controles necesarios para asegurar un nivel de seguridad adecuado, y mantener el riesgo por debajo de los niveles aceptados.
- La confidencialidad de la información debe garantizarse en todo momento.
- La integridad de la información debe asegurarse a través de todos los procesos que la gestionan, procesan y almacenan.
- La disponibilidad de la información debe garantizarse mediante las adecuadas medidas de respaldo y continuidad del negocio.

- Todo el personal con responsabilidades en materia de Seguridad de la Información debe disponer de la adecuada formación y concienciación con el establecimiento de un Plan de Formación, así como una correcta definición de roles y responsabilidades.
- Todo incidente o debilidad que pueda comprometer o haya comprometido la confidencialidad, integridad y/o disponibilidad de la información debe ser registrado y analizado para aplicar las correspondientes medidas correctivas y/o preventivas.
- Todos los contratos y/o acuerdos formalizados con empresas colaboradoras que impliquen un acceso a cualquier activo, provisión de servicio, conocimiento o información de la Compañía deben incluir cláusulas relativas a la propiedad intelectual de la Compañía, materia de privacidad, protección de datos de carácter personal y medidas de seguridad mínimas.
- Los proveedores de la Compañía deben ser revisados y analizados periódicamente, incluyendo aquellos nuevos riesgos identificados que puedan materializarse a partir de estos servicios y revisiones de cumplimiento normativo.
- Todo el personal de la Compañía, incluyendo a la Alta Dirección debe participar en procesos periódicos de formación para garantizar el cumplimiento de las Directrices y Responsabilidades recogidas en el presente documento.
- El acceso físico a los recursos a través de los cuales es mantenida y tratada la información, así como a cualquier edificio propiedad de la Compañía, debe contar con las oportunas medidas de control y salvaguardas que limiten accesos indebidos o no autorizados.

3.2. Procesos de gestión y mitigación

A continuación, se detallan los procesos principales sobre los que se desarrollarán las actividades de gestión:

- Seguridad en Recursos Humanos.
- Gestión de Activos.
- Control de Accesos.
- Gestión de Identidades.
- Cifrado y criptografía.
- Gestión de proyectos de TIC.
- Seguridad Física y Ambiental.
- Gestión de la capacidad y el rendimiento.
- Gestión de vulnerabilidades y parches.
- Seguridad de los datos y sistemas.
- Registro.
- Gestión de cambios en las TIC.
- Gestión de seguridad en las redes.
- Seguridad de la información en tránsito.
- Comunicación y Operación de Seguridad.
- Adquisición, Desarrollo y Mantenimiento de Sistemas.
- Cumplimiento, Auditorías y Revisión de la Seguridad
- Gestión de Proveedores.

- Seguridad en entornos Cloud.
- Formación y Concienciación.
- Gestión de Incidentes de Seguridad de la Información.
- Gestión de la Resiliencia TI.
- Gestión de la Continuidad.
- Datos de Carácter Personal.
- Código de conducta telemática: Es el documento que establece las directrices de seguridad que todo el personal de la organización tiene la obligación de conocer y cumplir.

3.3. Gestión y registro de incidentes de seguridad

Los incidentes relacionados con las TIC son objeto de un seguimiento, un tratamiento y una respuesta coherentes e integrados, a fin de asegurarse de que se identifiquen, se documenten y se aborden las causas subyacentes para evitar que se produzcan. Así mismo serán evaluados y notificados a la autoridad competente en caso de que sean considerados graves.

El registro de incidentes es un elemento fundamental del proceso de gestión de los riesgos tecnológicos y de la seguridad de la información (incluyendo seguridad física), ya que aporta información relevante sobre la materialización del riesgo y facilita, mediante su análisis, la toma de decisiones sobre su mitigación y control. Los incidentes de seguridad serán tratados bajo las premisas de la Política de Seguridad de la Información.

La información relativa a registro de incidentes de seguridad (a excepción de la cuantificación de la pérdida), así como sus impactos deberán ser reportados al menos semestralmente por el CISO en el Comité de Seguridad y en el Comité de Riesgos.

3.4. Principios de ciberseguridad en Inteligencia Artificial (IA)

Así como la Inteligencia Artificial es clave para diseñar y ejecutar los servicios de ciberseguridad, estos son cruciales a la hora de acometer la protección de los sistemas y aplicaciones de IA.

Partiendo de esta base, debemos señalar que, a la hora de abordar los riesgos de seguridad de la IA, hay que diferenciar entre:

- Las amenazas dirigidas a los sistemas de IA.
- El uso malicioso de herramientas de IA para poner en marcha ciberataques contra software y sistemas empresariales o contra particulares.

SCA manifiesta un claro compromiso por abordar estos aspectos teniendo en cuenta los siguientes principios:

- Dar cumplimiento, en los plazos exigibles y en aquello que se de aplicación en la actividad de la Compañía, a las prevenciones contenidas en el Reglamento (UE) 2024/1689, de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de Inteligencia Artificial.
- Securizar las aplicaciones y la infraestructura IT, escondiendo los parámetros del modelo, para protegerlo frente a los ataques.

- Fortalecer la protección de los nuevos desarrollos ligados a la IA.
- Gestionar de forma adecuada los problemas de sesgos en los sistemas de IA.
- Afrontar los riesgos asociados a la IA generativa.
- Hacer frente a los problemas de seguridad vinculados a la evasión, extracción de modelos, disponibilidad de los sistemas, etc.
- Analizar y monitorear monitorizar la compleja superficie de ataque de los sistemas de IA.
- Tener en consideración los riesgos vinculados a las tecnologías de IA desarrolladas por terceros.

3.5. Reporte e Informe de las Actividades

El CISO reportará:

- Al Comité de Riesgos, a la Comisión de Auditoría y, posteriormente, al Consejo de Administración, con carácter ordinario y una periodicidad semestral los siguientes aspectos:
  - Seguimiento de la Estrategia de Seguridad aprobada.
  - En el marco del Plan de la Dirección de. Seguridad Digital: los avances relevantes en el desarrollo de las iniciativas encaminadas a implementar y desarrollar esta política.
  - En el marco de los procesos de gestión y control de los riesgos TIC como primera línea: resultados de las distintas actividades realizadas y de los hechos significativos observados y estado de situación de las recomendaciones emitidas.
  - En su caso, los incidentes de seguridad (u operativos que hayan afectado a la tecnología y seguridad de la Información) más relevantes, incluyendo, al menos, del efecto, la reacción y los controles adicionales que deben definirse en razón de los incidentes.
- Al Comité de Dirección, con una periodicidad mínima cada dos meses, con los avances relevantes en iniciativas desde un punto de vista de cumplimiento, técnico, de detección y de recuperación; hitos alcanzados que han permitido el incremento de la madurez de los Criterios de Seguridad de la Información durante el período, y otros indicadores que muestren el estado de la seguridad y la resiliencia de la infraestructura de la Compañía.
- A los Órganos Supervisores, cuando así sea requerido por cualquier circunstancia por el supervisor.

4. Aspectos organizativos

Se llevará a cabo una gestión organizada de la Seguridad de la Información, teniendo en cuenta las necesidades en cuanto a roles y responsabilidades en materia de Seguridad de la Información. Caben recalcar las siguientes responsabilidades y funciones dentro del área de Seguridad Digital:

- Con objeto de promover y conseguir los objetivos definidos de Seguridad de la Información, la Función de Seguridad de la Información, y su titular, operará bajo la responsabilidad última del Consejo de Administración.

- Esta estructura permite a la Función reportar y asesorar directamente al Consejo de Administración cuando así sea necesario o requerido para ello conforme a las funciones que tiene atribuidas en esta política, desarrollando su labor libre de influencias que comprometan su capacidad para desempeñar sus tareas de modo objetivo, imparcial e independiente.

Sin perjuicio de lo anterior, el responsable de la Función se encuentra en una Dirección bajo la dependencia jerárquica de la Dirección de Tecnología y Transformación Tecnológica, garantizándose su independencia y objetividad de cualquier proceso de desarrollo y operaciones de TIC. Por tanto, dentro de la Dirección de Seguridad Digital y Continuidad, la función clave es el CISO (Chief Information Security Officer), Director de la Seguridad de la Información o Responsable de Seguridad de SegurCaixa Adeslas. El detalle de las funciones del área se encuentra detallado en el documento Norma de Gobierno de la Seguridad, CN y RTI.

Anexo I: 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).
- 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 - Gestión de la Seguridad de la Información.
- ISO/IEC 27002 - Tecnología de la información - técnicas de seguridad - código de prácticas para los controles de seguridad de la información.
- ISO/IEC 27005 - Seguridad de la información, ciberseguridad y protección de la privacidad.
- ISO/IEC 27017 - Controles de Seguridad para Servicios Cloud.
- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección 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).
- 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 Cybersecurity Framework 2.0. Agosto 2023.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CO).

Fin de documento: PL02602 Política de Seguridad de la Información