POLÍTICA DE SEGURIDAD

SegurCaixa Adeslas

Índice

La presente Política de Seguridad es un extracto de la Política de Gestión y Control del Riesgo Tecnológico y Seguridad de la Información, aprobada en Consejo de Administración.

Política de Seguridad

Fecha de aprobación:	30 de noviembre de 2021
Responsable de edición y revisión	D.A. Seguridad Digital y Continuidad
Estado	Vigente

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	30/11/2021	Edición	D.A. Seguridad Digital y Continuidad	Comité de Seguridad

1. Introducción

La presente política es un extracto de la Política que 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 aplicables a cualquier persona o Compañía que acceda a activos de la información de SegurCaixa Adeslas, incluyendo a terceras partes.

La presente Política es un extracto de la Política de Gestión y Control del Riesgo Tecnológico y de la Seguridad de la Información aprobada por el Consejo de Administración de la Compañía.

1.1. Objetivo 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 del riesgo operacional y de seguridad de las tecnologías de la información y de las comunicaciones (en adelante también “TIC”).

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, así como 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.

SegurCaixa Adeslas se compromete a asegurar todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, con procesos orientados a la gestión del riesgo tecnológico, garantizando siempre el cumplimiento de las distintas normativas y leyes aplicables y preservando en todo momento las dimensiones básicas de la Seguridad de la Información, bajo un proceso de mejora continua:

- Confidencialidad: Propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos de información.
- Disponibilidad: Propiedad de ser accesible y utilizable por una entidad autorizada.

1.2. Principios de gestión de riesgos tecnológicos y de la seguridad de la información

Mediante la presente política, se declaran como principios generales de la gestión de riesgos tecnológicos, así como de la seguridad de la información el compromiso de la Compañía hacia los siguientes objetivos:

- 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 riesgo residual (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.
- Garantizar la confidencialidad, integridad y disponibilidad de toda la información procesada o albergada en el ámbito de la compañía.

De cara a establecer las herramientas para la consecución de dichos principios, las áreas responsables podrán establecer normativa interna más específica tanto sobre la seguridad de la información como sobre la gestión de riesgos tecnológicos. 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.

1.3. Ámbito de aplicación

El ámbito de aplicación de esta Política de Seguridad abarcará a cualquier persona o empresa que acceda a cualquiera de los sistemas de información de SegurCaixa Adeslas.

Todas las partes implicadas se comprometen a cumplir y a hacer cumplir todos los principios de seguridad que el Consejo de Administración ha establecido a través de la aprobación de la Política de Control y Gestión del Riesgo Tecnológico y Seguridad de la Información, con el fin de garantizar la protección de la información y la continuidad del negocio en todo momento.

Entra en vigor el mismo día de su publicación, siendo revisada periódicamente por el Comité de Seguridad y estando alineada con la Política de Control y Gestión del Riesgo Tecnológico y Seguridad de la Información.

2. Estrategia, procesos y procedimientos

La gestión del riesgo tecnológico y de la seguridad de la información (en adelante “riesgos TIC”), es un proceso integral que implica y afecta en su aplicación y desarrollo a toda la organización y a todos los niveles, comprendiendo la identificación, el análisis, la evaluación, el tratamiento o respuesta, la mitigación y el control de los riesgos.

El modelo de gestión de los riesgos TIC se fundamenta sobre las pautas establecidas en la Política de gestión del riesgo operacional. De forma complementaria contemplará los siguientes aspectos:

- Aspectos organizacionales y de atribución de responsabilidades.
- Diseño de los procesos operativos y el mantenimiento de los procedimientos correspondientes que sean reflejo de los principios a seguir en la gestión de los riesgos tecnológicos y de seguridad de la información

- Proceso de gestión de riesgos que incluye:
  - la Identificación y categorización de los riesgos,
  - el análisis y la evaluación de los riesgos, así como el establecimiento de los controles que permitan reducir la misma a los niveles deseados,
  - la gestión del riesgo tecnológico,
  - la supervisión y monitorización,
  - el registro de incidentes de seguridad, y
  - el reporte e informe de las actividades.

Este modelo de gestión deberá quedar reflejado en el "Cuerpo Normativo de Riesgos Tecnológicos y de Seguridad de la información".

2.1. Organización y Responsabilidades

El Consejo de Administración de SegurCaixa Adeslas aprueba la Política de Gestión y Control del Riesgo Tecnológico y de la Seguridad de la Información y define la organización y responsabilidades en materia de la Seguridad de la Información.

2.2. Cuerpo Normativo de Seguridad

En base a la Política de Control y Gestión del Riesgo Tecnológico y Seguridad de la Información, y con la finalidad de cumplir sus objetivos, se fijarán las medidas concretas de índole técnica y organizativa necesarias a aplicar en los Sistemas de Información y cualquier recurso que contenga información de SegurCaixa Adeslas, de aplicabilidad para cualquier persona o empresa que acceda a cualquiera de los sistemas de información de SegurCaixa Adeslas Estas medidas se desarrollarán en diferentes documentos que a continuación se especifican:

2.2.1. Normas de Seguridad de la Información.

Conjunto de documentos de carácter normativo que soportan los objetivos recogidos en la Política de Control y Gestión del Riesgo Tecnológico y Seguridad de la Información. Las normas describen lo que se debe realizar en cada sección o ámbito, así como los activos que se quieren proteger y las funciones de prevención y control asociadas.

2.2.2. Procedimientos de Seguridad de la Información.

Conjunto de documentos que recogen los detalles y actividades de las medidas de Seguridad de la Información expuestas en las Normas. En cada Procedimiento deberán indicarse los registros documentales o evidencias resultantes de su ejecución por las Áreas de SegurCaixa Adeslas y partes interesadas, con el objeto de garantizar el correcto desempeño y seguimiento de éstos, así como su posterior revisión o auditoría de seguridad.

2.2.3. Instrucciones Técnicas de Seguridad de la Información.

Conjunto de documentos que recogen los manuales específicos de uso y funcionalidades de las herramientas y procesos mencionados en los Procedimientos.

2.3. Principios de Seguridad de la Información.

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

Este marco de Principios de Seguridad de la Información presenta los objetivos de Seguridad de la Información alineados con la estrategia de la Compañía, tales como 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.

A continuación, se establecen los Principios de Seguridad de la Información que soportan 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.
- 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 la Seguridad de la Información, abarcando al menos: factores internos y externos, proveedores y otras entidades y amenazas internas y externas.
- 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.
- 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 y a los miembros del Consejo de Administración, 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.

Para la consecución de los objetivos de esta Política, la Compañía establece una estrategia de análisis y tratamiento sobre los riesgos que puedan llegar a afectarle, manteniendo una definición de riesgo aceptable y umbrales de tolerancia claros en la Política de Gestión de Riesgos.

2.4. Procesos de Seguridad de la Información.

A continuación, se detallan los procesos principales sobre los que se desarrollarán las actividades de la Función, desde un enfoque mayoritariamente preventivo y considerando controles reactivos.

2.4.1. Seguridad en Recursos Humanos.

Los empleados de SegurCaixa Adeslas, externos o internos, deben conocer y comprender sus responsabilidades y funciones con respecto a la Seguridad de la Información, además de tener una descripción adecuada de su puesto de trabajo y adecuados términos de contratación.

Deberán existir medidas en materia de Seguridad que deberán ser consideradas en todo el proceso de selección de personal, en la elaboración de contratos y durante la etapa laboral, a fin de reducir los riesgos de manipulación, robo, fraude o uso inadecuado de la información. Una vez finalizada la etapa laboral también se deberán considerar medidas de finalización de contrato y baja de usuarios.

Será competencia de los miembros de la Compañía la obligación de obrar con diligencia con respecto al material y a la información, debiéndose encargar de que dicha información no caiga en poder de personal no autorizado.

2.4.2. Gestión de Activos.

Los activos tanto tangibles como intangibles de SegurCaixa Adeslas deben estar registrados, etiquetados, clasificados y deben contar con un responsable asignado.

Se deberán establecer un conjunto de medidas para el uso aceptable de los activos de la Compañía y para la clasificación, etiquetado y manipulado de los activos de información, manteniendo así su integridad y protegiéndolos de fugas, borrados accidentales o accesos no autorizados.

Toda la información corporativa deberá clasificarse y etiquetarse para facilitar los procesos de control de acceso, custodia y monitorización. En base al nivel de clasificación de la información, la Compañía establecerá medidas y controles preventivos: cuanto más confidencial se considere la Información, más restrictivos deberán ser dichos controles.

Asimismo, deberá existir un inventario actualizado de activos que detalle el responsable o propietario de cada activo. También se deberán definir las bases para el buen uso de los activos de la Compañía, de cara a mantener un nivel de seguridad adecuado y mitigar cualquier riesgo que pueda materializarse debido un mal uso de estos, además de agilizar actividades de contención de un incidente de seguridad que pueda afectar a un activo.

2.4.3. Control de Accesos.

El control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los Sistemas de Información.

Todos los Sistemas de Información deberán de contar con un sistema de control de acceso. Asimismo, todos los accesos deberán ser controlados y ningún usuario podrá acceder a un Sistema de Información sin la aprobación de su responsable.

De cara a garantizar estas medidas de seguridad los usuarios no podrán ser compartidos y todos ellos serán inicialmente asignados mediante la política de mínimo privilegio, otorgando únicamente los privilegios mínimos necesarios para desempeñar su función posteriormente.

Se deberán revisar periódicamente los derechos de acceso otorgados a todos los usuarios para detectar y eliminar aquellos que ya no sean necesarios.

Con el objetivo de facilitar la identificación e investigación de actividades anómalas que puedan afectar a la seguridad de sus sistemas, la Compañía deberá registrar y monitorizar todas las actividades de los usuarios, en especial, las de los usuarios privilegiados. Dichos registros de acceso se protegerán contra modificaciones o borrados no autorizados y serán conservados durante un periodo de tiempo establecido.

Las conexiones remotas deberán realizarse a través de una conexión VPN segura otorgada por la propia entidad, la cual deberá ser aprobada, registrada y auditada por la D.A. de Seguridad Digital y Continuidad.

2.4.4. Cifrado.

Deberá diferenciarse entre el cifrado de información en tránsito, y cifrado de información en reposo. Todos los métodos de cifrado utilizados en SegurCaixa Adeslas deberán de ser reconocidos como no vulnerables por las buenas prácticas establecidas por la D.A. de Seguridad Digital y Continuidad. Las claves de cifrado de estos algoritmos deberán de ser almacenadas en aquellos sistemas corporativos destinados a dicho fin.

2.4.5. Seguridad Física y Ambiental.

Las instalaciones y oficinas, al igual que los activos tangibles localizados en estas, pueden ser vulnerables a amenazas ambientales, y requieren de una capa adicional de seguridad que considere no solo la información almacenada, sino también la integridad física de los mismos.

Se deberán identificar y establecer medidas de control físicas para proteger los activos de información para evitar incidentes que afecten a la integridad física y lógica de la información y a la disponibilidad de las infraestructuras. Estas medidas de control deberán estar alineadas con el nivel de riesgo previamente identificado que afecte a los datos y a la información, y podrán ser evaluadas con el compromiso de garantizar la confidencialidad, integridad y disponibilidad de los mismos.

Los espacios físicos donde se ubiquen los Sistemas de Información o destinados al ámbito laboral deberán ser adecuadamente protegidos mediante controles de acceso perimetrales, sistemas de vigilancia y medidas preventivas, como sistemas antiincendios, de manera que puedan evitarse incidentes de seguridad y accidentes ambientales (incendios, inundaciones, cortes de suministro eléctrico, etc.).

2.4.6. Comunicación y Operación de Seguridad.

SegurCaixa Adeslas debe asegurar la operación correcta y segura de las instalaciones de procesamiento de información y de la infraestructura de redes.

Todos los Sistemas de Información deberán contar con medidas de seguridad para optimizar su funcionamiento y madurez, incluyendo copias de seguridad periódicas que permitan restablecer cualquier sistema o activo garantizando el menor impacto sobre sus datos. Así

mismo, se deberán gestionar y controlar las redes de manera adecuada, a fin de protegerlas frente a amenazas y mantener la seguridad de las mismas. Los sistemas y aplicaciones que utilicen la red, incluido el control de acceso a la red, deberán contar con medidas de protección para la transferencia e intercambio de información.

Se deberán establecer medidas de seguridad para la correcta gestión de los procesos de cambio y de capacidad, permitiendo así una planificación adecuada de los Sistemas de Información.

Finalmente, y con el objetivo de facilitar las tareas de auditoría y la trazabilidad de los sistemas, se deberá mantener un registro actualizado de todos los cambios y eventos llevados a cabo en los Sistemas de Información. Éstos deberán disponer de generación de registros o logs, que puedan ser correlados como eventos por parte de Seguridad Digital con objeto de identificar preventivamente cualquier vector de amenaza, o permita, reactivamente, analizar la causa raíz de un incidente de seguridad materializado. El detalle de estos registros será directamente proporcional a la criticidad del activo, aplicación, entorno o servicio.

2.4.7. Adquisición, Desarrollo y Mantenimiento de Sistemas.

SegurCaixa Adeslas debe garantizar que la Seguridad de la Información es una parte integral del ciclo de vida de los Sistemas de Información, ya sean propios o de terceros. Los Sistemas de Información incluyen sistemas operativos, infraestructura, aplicaciones de negocio, servicios y desarrollos propios.

Toda la adquisición, desarrollo y mantenimiento de sistemas deberá contar con unos requisitos mínimos de seguridad necesarios para el desarrollo de software, así como para su puesta en producción o conexión a la infraestructura existente de SegurCaixa Adeslas. Además, el desarrollo posterior y la gestión se incluirán cuando el software se haya cargado en el entorno de producción, incluidas las pruebas, el seguimiento de los cambios e inventario.

Cada unidad de negocio de la Compañía debe tener en cuenta la Seguridad de la Información en sus procesos y procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

2.4.8. Revisiones, evaluaciones y pruebas de la Seguridad de la Información.

Con el propósito de garantizar los niveles y objetivos de seguridad definidos, se deberá establecer una planificación exhaustiva y un calendario de pruebas y revisiones periódicas de seguridad, de forma que se identifiquen todas aquellas vulnerabilidades que pudiesen encontrarse presentes en la arquitectura de seguridad, los sistemas, los proveedores, o los desarrollos en SegurCaixa Adeslas.

Asimismo, para validar la idoneidad de las medidas de Seguridad de la Información desplegadas, la Compañía establecerá y aplicará un marco de pruebas de seguridad, y garantizará que este contemple las amenazas y vulnerabilidades identificadas en el proceso de identificación y evaluación de riesgos de seguridad, así como escenarios de posibles ataques relevantes y conocidos.

En el caso de activos, servicios o plataformas externalizadas en proveedores, clasificados como críticos, por Negocio o por la D.A. de Seguridad Digital y Continuidad, las pruebas podrán realizarse al menos anualmente. Para aquellos activos no críticos podrán realizarse

pruebas periódicas siguiendo un enfoque basado en el riesgo y al menos una vez cada tres años.

La D.A. de Seguridad Digital y Continuidad monitorizará y evaluará los resultados de las pruebas de seguridad, y actualizará sus medidas de seguridad de acuerdo a estos, con los plazos definidos en la normativa referente a la gestión de vulnerabilidades de seguridad.

2.4.9. Gestión de Proveedores.

SegurCaixa Adeslas externaliza una parte de sus servicios a proveedores externos, confiando así en las medidas de seguridad de otras empresas. Estas deben ser supervisadas y analizadas periódicamente para asegurar el correcto cumplimiento con lo dispuesto en el Cuerpo Normativo de la Compañía, a través de procesos de revisión bajo demanda y mediante el seguimiento del cumplimiento de los niveles de servicio de seguridad acordados.

Se deberán establecer un conjunto de medidas para gestionar los servicios derivados de proveedores, realizando análisis periódicos de cada proveedor y evaluando la criticidad de los mismos, teniendo en cuenta la sensibilidad de los datos que se traten y la naturaleza del servicio provisionado.

Cuando se utilicen servicios de terceros o se ceda información a terceros, se les hará partícipes de esta Política de Seguridad y del Cuerpo Normativo de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, bajo supervisión y validación de SegurCaixa Adeslas.

Para conseguir este principio de seguridad, se establecerán marcos periódicos de evaluación de los proveedores, según su criticidad y el riesgo identificado de cada uno, mediante la auditoría y revisión de sus requerimientos contractuales, la monitorización de los niveles de servicio y las medidas de seguridad implantadas por dicho proveedor para proteger los activos de información de SegurCaixa Adeslas.

2.4.10. Seguridad en entornos Cloud.

Toda información perteneciente a la Compañía que se encuentre almacenada en servidores Cloud (información alojada en Internet) deberá ser tratada y procesada según los requisitos especificados en las normativas y estándares de seguridad que sean de aplicación sobre la Compañía, debiendo diferenciarse entre las medidas de seguridad para Cloud Pública y las medidas de seguridad para Cloud Privada.

2.4.11. Cumplimiento Regulatorio y de Seguridad.

SegurCaixa Adeslas se compromete a dotar de los recursos necesarios para dar cumplimiento a toda legislación y regulación aplicable a la actividad de la Compañía en materia de Seguridad de la Información.

En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable, incluyendo los requisitos legales, reglamentarios y contractuales sobre el uso del material con derechos de propiedad intelectual y sobre el uso de productos de software patentados. Así mismo, se deberá garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes.

Adicionalmente, se deberán llevar a cabo revisiones y auditorías periódicas de cumplimiento de la Seguridad de la Información por personal independiente a la Compañía.

2.4.12. Formación y Concienciación.

Todos los miembros de la Compañía, proveedores y usuarios de terceros deben recibir una concienciación adecuada sobre las políticas y los procedimientos de la organización. Los miembros de la organización, adicionalmente, requieren de una formación adecuada a sus funciones, responsabilidades y habilidades.

Deberán instaurarse y aplicarse programas periódicos de sensibilización sobre Seguridad de la Información, con el objeto de concienciar sobre los distintos riesgos de seguridad existentes y cómo deben ser tratados, a fin de garantizar que reciben la formación necesaria para cumplir con sus obligaciones y responsabilidades y reducir los errores humanos, los robos, el fraude, los usos indebidos y las pérdidas.

Todos los miembros de la Compañía atenderán a una sesión de concienciación en materia de Seguridad TIC al menos una vez al año. Así mismo, se establecerá un programa de concienciación continua para todos los miembros de la Compañía, en particular a los de nueva incorporación.

Las personas que hagan uso o accedan a los Sistemas de Información recibirán formación para el manejo seguro de los sistemas en medida de sus funciones de trabajo y/o el puesto que ocupen. La formación será de obligado cumplimiento.

Adicionalmente, se garantizará que el personal de terceros y los proveedores de servicios estén adecuadamente concienciados y formados en materia de seguridad.

2.4.13. Gestión de Incidentes de Seguridad de la Información.

Un incidente de seguridad consiste en cualquier evento que pueda comprometer la confidencialidad, integridad y/o disponibilidad de la información, así como afectar a la consecución de los objetivos de la Compañía.

La presente Política establece la obligación y responsabilidad de todos los miembros de la Compañía, así como de las empresas que prestan servicio a la misma, de la identificación y notificación al Responsable de Seguridad de cualquier incidente que pudiera comprometer la Seguridad de los activos de información de SegurCaixa Adeslas.

Para minimizar el impacto de un incidente o materialización de amenaza, se seguirá una estrategia de contención y resolución de incidentes de seguridad establecida por la Compañía, efectuando una comunicación constante con los distintos Departamentos interesados de SegurCaixa Adeslas (Oficina de Privacidad, etc.).

Para ello, deberán establecerse planes de comunicación interna eficaces, incluidos los procedimientos de elevación a otro nivel y notificación, que también abarquen las reclamaciones de los clientes relacionadas con la seguridad, para garantizar que los incidentes con un efecto adverso potencialmente elevado sobre sistemas y servicios de TI esenciales se notifican a la Alta Dirección.

Los incidentes críticos/relevantes que eleven el perfil de riesgo de SCA o cualquier entidad del grupo deben ser informados de manera inmediata a la Dirección de Control de Riesgos, Comité de Riesgos y Comisión de Auditoría.

Se deberá reportar y comunicar al Consejo de Administración, según los mecanismos definidos a tal efecto en el epígrafe 4.5 de la presente Política, al menos, del efecto, la reacción y los controles adicionales que deben definirse en razón de los incidentes, además de otra información relevante, según definido en los Principios de Seguridad de la Información.

2.4.14. Gestión de la Resiliencia TI.

Los activos, sistemas y procesos de SegurCaixa Adeslas necesitan disponer de capacidad de resiliencia, es decir, operar con el menor impacto posible ante un cambio no planificado o una alteración como, por ejemplo, un incidente de seguridad, garantizando su recuperación al estado inmediatamente anterior.

Para ello se deberán crear y mantener sistemas y herramientas resilientes que minimicen el impacto del riesgo, identificando de forma continua todas las fuentes de riesgo y estableciendo medidas de protección y prevención.

Adicionalmente, se deberán implantar políticas específicas y exhaustivas de continuidad de la actividad, en conjunción con el Área de Continuidad de la Compañía, y planes de recuperación en caso de catástrofe. Éstos son necesarios para una rápida recuperación tras incidentes relacionados con los Sistemas de Información, como ciberataques, limitando los daños y dando prioridad a la reanudación segura de las actividades.

Finalmente, se deberán ejecutar pruebas periódicas para comprobar el estado de preparación y asegurarse de la detección de deficiencias en los sistemas, así como de la rápida aplicación de medidas correctoras. Los resultados de las pruebas deberán documentarse y las deficiencias identificadas como resultado de las pruebas habrán de analizarse, tratarse y notificarse al Consejo de Administración.

2.4.15. Gestión de la Continuidad.

De acuerdo a la Política de Continuidad de Negocio y respondiendo a requerimientos de calidad y buenas prácticas, se ha desarrollado un Plan de Continuidad de Negocio, como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios críticos y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la entidad actúe en caso de ser necesario.

2.4.16. Datos de Carácter Personal.

SegurCaixa Adeslas tratará los datos de carácter personal de acuerdo con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, el Reglamento (UE) 2016/679 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, así como en el resto de normas o disposiciones legales que puedan resultar de aplicación.

Todos los Sistemas de Información de la Compañía se ajustarán a los niveles de seguridad requeridos por dicha normativa teniendo en cuenta la naturaleza y la finalidad de los tratamientos de dichos datos de carácter personal y, de forma particular, en lo que respecta a las obligaciones de registro de actividades, evaluación de impacto, selección de proveedores y comunicación de brechas de seguridad, se estará a lo recogido por SegurCaixa Adeslas en su Manual de Protección de Datos y en su normativa de desarrollo.

2.4.17. Gestión de Riesgos de Seguridad.

SegurCaixa Adeslas debe considerar los riesgos a los que sus activos están expuestos, realizando una evaluación de riesgos periódica y exhaustiva, desde un punto de vista de Seguridad de la Información, identificando los distintos impactos considerando las dimensiones básicas confidencialidad, integridad y disponibilidad.

Esta evaluación de riesgos de seguridad deberá identificar, cuantificar y priorizar los riesgos frente a los criterios para la aceptación del riesgo y los objetivos pertinentes para la organización definidos por la D.A. de Seguridad Digital y Continuidad, que actúa en este caso como primera línea de defensa, siendo la responsable de identificar, evaluar y gestionar el riesgo, diseñando y ejecutando los controles necesarios para mitigarlos y mantenerlos dentro de los niveles de apetito al riesgo y/o límites establecidos. Igualmente, será responsable de mantener una adecuada documentación y registro de los procesos, de los controles y de la ejecución de los mismos y de informar a la Dirección y a las Funciones clave sobre cualquier evento o cambio significativo que se produzca con impacto en los sistemas de control interno y de riesgos.

La evaluación de riesgos de seguridad, por tanto, se convierte en una fuente de información básica para la ejecución de las propias funciones de la D.A. de Seguridad Digital y Continuidad y su compromiso con la mejora continua, y constituye una pieza fundamental para la gestión de riesgos.

La D.A. Seguridad Digital y Continuidad como primera línea de defensa, deberá realizar análisis de riesgos de seguridad sobre todos los activos sujetos a la presente Política de Seguridad y a las amenazas a los que están expuestos, generando resultados repetibles y comparables, a partir de un catálogo de amenazas identificado para SegurCaixa Adeslas y considerando como medidas de mitigación del riesgo las medidas de seguridad o salvaguardas existentes en el momento del análisis. Estos análisis de riesgos deberán repetirse sobre un entorno, servicio o activo cuando cambie de forma significativa la información manejada, cuando ocurra un incidente grave de seguridad, o cuando se reporten vulnerabilidades graves.

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.

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).
- Guía Técnica 2/2017 de la Dirección General de Seguros y Fondos de Pensiones sobre cuestiones en materia de Sistema de Gobierno.
- ISO/IEC 27001:2013 "Information technology - Security techniques - Information security management systems - Requirements".
- ISO/IEC 27002:2013 "Information technology - Security techniques - Code of practice for information security controls".
- ISO/IEC 27005:2018 "Information technology - Security techniques - Risk Management of Information Security".
- ISO/IEC 27017:2015 “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.
- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Fin de documento: Extracto PL02401_Politica de Seguridad.docx