bankinter

SGP02. Extracto integrado de políticas de Seguridad y Continuidad de Negocio del Grupo Bankinter

Índice

Contenido del documento

1. Objetivos

1.1 Objetivo de la PSI

El propósito de la **Política de Seguridad de la Información del Grupo Bankinter**, en adelante, PSI, es establecer un marco normativo para la seguridad de la información que nos permita identificar, desarrollar e implantar las medidas técnicas y organizativas necesarias para garantizar la seguridad de la información y de los sistemas que la gestionan, de acuerdo a análisis de riesgos, buenas prácticas de la industria y los requerimientos legales y contractuales a los que está obligado el Grupo Bankinter.

1.2. Objetivo de la Política de Continuidad de Negocio

El propósito de la **Política de Continuidad de Negocio del Grupo Bankinter** (incluyendo el SGCN - *Sistema de Gestión de la Continuidad de Negocio*) es establecer un marco apropiado a las características de Bankinter (naturaleza, escala, complejidad, criticidad de las actividades, etc.) que repercuta directamente en el entorno operativo, dependencias y cultura del banco, y con el que se consiga identificar, desarrollar, implantar, operar, mantener, revisar y probar las medidas de continuidad necesarias para garantizar el correcto funcionamiento tanto de los Planes de Continuidad de Negocio establecidos como de los Sistemas que gestionan la Continuidad de negocio de Bankinter ante la aparición de un incidente disruptivo.

Con todo ello lo que se pretende es proteger a nuestros colaboradores, clientes y marca manteniendo en un nivel aceptable los servicios críticos prestados a nuestros clientes a la vez que se da una respuesta adecuada a contingencias que puedan estar o no previstas adaptándose a los cambios del entorno operativo.

2. DECLARACIÓN DE PRINCIPIOS

2.1. Principios de Seguridad de la Información:

"La **información** es considerada como un activo de gran importancia para el Grupo Bankinter; ésta ha de ser **precisa**, **oportuna** y **pertinente** y es esencial para que nuestro negocio sea eficaz. Por ello se establecen protocolos de seguridad, los cuales deben ser conocidos, aceptados y cumplidos por todos y cada uno de los empleados, con el fin de asegurar la protección de la información. De esta forma las obligaciones de Bankinter con los clientes, los socios, los empleados, los organismos gubernamentales y otras partes interesadas se cumplirán".

La Dirección reconoce su **compromiso con la mejora continua** y su responsabilidad en apoyar los protocolos de seguridad que permitan minimizar los riesgos a los que se encuentra expuesta la información en la consecución de los objetivos estratégicos del negocio. Por tanto, se reconoce la importancia de las medidas de control para minimizar los riesgos sobre la información derivados de amenazas tales como: errores, fraudes, malversaciones, sabotajes, terrorismo, extorsiones, espionaje industrial, violaciones de intimidad, interrupciones de servicio y desastres naturales entre otras.

La seguridad de la información debe considerarse como una parte de la operativa habitual, no como un extra añadido

2.2. Principios de Continuidad de Negocio:

La Política de Continuidad de Negocio se define en términos de objetivos de la organización y de sus obligaciones asegurando que:

- Es apropiada para el propósito de la Organización definido en sus objetivos estratégicos.
- Proporcionará un marco para establecer los objetivos de Continuidad perseguidos.
- Plasmará el compromiso para satisfacer los requisitos y requerimientos aplicables, previamente identificados e incluidos en el análisis de impacto, así como la mejora continua del sistema verificable en sus revisiones y auditorias.
- Impulsará la Gestión de la Continuidad de Negocio, estableciendo escenarios generales de Indisponibilidad (Instalaciones, RRHH, Tecnología y Servicios prestados por terceros).

3. OBJETIVOS ESTRATÉGICOS

3.1. Seguridad de la Información

El desarrollo y la implantación de las medidas técnicas y organizativas de la PSI están orientados a la protección de las principales dimensiones sobre las que se soporta la seguridad de la información:

- **Confidencialidad**: Garantizar un acceso limitado a la información estando sólo accesible por aquellos que lo precisan, así como la generación de los registros o trazas de eventos que aseguren su auditabilidad.
- **Integridad**: Garantizar que la información sólo es tratada en la forma y modo que se ha estipulado, debiendo ser su contenido siempre completo o exacto, además de auténtico.
- **Disponibilidad**: Garantizar que la información esté disponible dónde y cuándo se necesita.

Sobre estas bases la Dirección de Bankinter establece **nueve objetivos estratégicos** para la protección de la seguridad de la información:

1. Proteger integralmente la información y activos de clientes, negocio y empleados.
2. Garantizar la continuidad de los servicios y procesos.
3. Alinear la seguridad con los objetivos de negocio y con la estrategia tecnológica de la compañía.
4. Gestionar de forma eficiente los Riesgos Tecnológicos.
5. Estar a la vanguardia en Seguridad TI en el sector financiero español.
6. Dar una respuesta eficaz a incidentes, mejorando de manera continua los procesos de seguridad, procedimientos, productos y servicios, así como los planes de recuperación.
7. Cumplir con los requisitos legales, de negocio y otros requisitos de los clientes (explícitos e implícitos) relacionados con la seguridad de la información, la privacidad y la protección de datos.
8. Fomentar la seguridad de la información dentro y fuera del Banco.
9. Garantizar la segregación de funciones en la atribución y desempeño de responsabilidades.

3.2. Continuidad de Negocio

La Dirección de Bankinter establece los siguientes objetivos estratégicos para mantener la continuidad de los procesos y servicios críticos:

1. La Dirección de Bankinter reconocerá la gestión de los riesgos claves para la continuidad de los procesos y servicios críticos de la Compañía.
2. La protección y seguridad del personal habrá de ser la primera premisa y será el objetivo prioritario.
3. Se nombrará un responsable de Continuidad de Negocio que velará por la consecución de los objetivos de Continuidad de Negocio establecidos en la organización.
4. Se nombrará representantes corresponsales con la debida experiencia para que formen parte de los Equipos de Continuidad, participen en los Planes de Continuidad y se responsabilicen del mantenimiento de los planes en nombre del Área.
5. Los Equipos de Continuidad garantizarán que los Planes de Continuidad son desarrollados, probados e implementados de forma adecuada, teniendo en cuenta todas las Áreas, proveedores y servicios externalizados críticos dentro del alcance.
6. Los Equipos de Continuidad gestionarán la Activación de los Planes de Continuidad, en base a la evaluación de Daños realizada por los Equipos de Coordinación y Evaluación. En caso de Activación de algún Plan, se notificará al Comité de Crisis, quien será el órgano más importante de todas las gestiones realizadas durante toda la situación de crisis (incluyendo la recuperación, la operación en contingencia y la vuelta a la normalidad).
7. Los Equipos de Continuidad garantizarán que los Planes de Continuidad velan de forma permanente, inequívoca y prioritaria por la salud, seguridad y bienestar de todo el personal que pudiera verse involucrado durante la contingencia.
8. Los Equipos de Continuidad garantizarán que los procesos críticos pueden ser recuperados dentro de los márgenes de tiempo requeridos en los Planes de Continuidad. La disponibilidad de los sistemas se asegurará mediante el uso de niveles apropiados de resiliencia, estrategias, objetivos de rendimiento y KPI's.
9. Las recuperaciones, tanto en los ámbitos de las TIC (Sistemas, Tecnología, etc), como del resto de elementos (personas, instalaciones, etc), se priorizarán en función de la criticidad de los procesos de Negocio, y de los elementos específicos, yendo del más al menos restrictivo, continuando con los elementos no críticos.
10. Los Equipos de Continuidad garantizarán que los Planes de Continuidad son mantenidos, actualizados, revisados, probados y, en su caso, mejorados de forma periódica, al menos anualmente y ante cambios significativos en premisas, personas, procesos, mercados, tecnología o estructura organizativa de Bankinter.

11. Los Equipos de Continuidad garantizarán que todo el personal de las Áreas de Negocio esté informado y cuente con las capacidades suficientes para el desempeño de las responsabilidades que le competen en el marco de la Continuidad de Negocio, mediante labores periódicas de formación, divulgación y pruebas de los Planes de Continuidad.
12. Los Equipos de Continuidad garantizarán Planes de Comunicación apropiados, tanto internos como externos, que serán revisados y mantenidos de forma periódica.
13. La Dirección dotará de presupuesto y recursos suficientes al marco de gestión de los Planes de Continuidad de Negocio para cumplir sus objetivos.
14. Todos aquellos responsables de la planificación de nuevos proyectos, así como de la operación de proyectos existentes incluirán en la planificación y presupuesto de estos los niveles requeridos de resiliencia e impacto en los Planes de Continuidad y disposiciones oportunas.
15. El Gobierno de la Continuidad de Negocio se detallará en un framework común para todas las filiales del Grupo Bankinter que abarcará todos los procesos de Gestión de la Continuidad de Negocio y sus interrelaciones.
16. La Dirección se asegurará de la promoción y divulgación de la capacidad de continuidad de negocio dentro de la cultura de Bankinter.

4. SISTEMAS DE GESTIÓN

Para garantizar el éxito en la implantación de la PSI y la Política de Continuidad de Negocio, así como la consecución de los objetivos estratégicos anteriores, Bankinter cuenta con el firme compromiso y apoyo de la Dirección para la implantación de dos sistemas de gestión:

- Sistema de Gestión de Seguridad de la Información (SGSI).
- Sistema de Gestión de Continuidad de Negocio (SGCN).

Estos se basan en dos estándares internacionales, la ISO/IEC 27001 Information security management y la ISO 22301 Societal security -- Business continuity management systems --- Requirements, respectivamente, y se encuentran certificados en base a un alcance específico y acotado por una entidad externa independiente.