POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS		
ESTADO DE REVISIÓN/MODIFICACIÓN DEL DOCUMENTO		
N.º Edición	**Fecha**	**Naturaleza de la Revisión**
00	17/05/2021	Edición inicial
01	13/02/2023	Revisión
02	11/07/2023	Modificación de alcance
03	20/06/2024	Revisión sin cambios

ELABORADO **Responsable de SIG**	**REVISADO** **Dirección**	**APROBADO** **CEO**
Antoni Grau	David Ariño	Xavier Costa Ran

MISIÓN CORPORATIVA

Desde su inicio en 1974, Grupo BC mantiene la esencia que siempre le ha caracterizado: la de una empresa cercana con sus clientes, capaz de adaptarse y generar modelos de negocio innovadores en cada paso de su camino.

Con trabajo, profesionalidad y cercanía, en Grupo BC ha conseguido convertirse en un referente de la externalización de servicios y procesos

Grupo BC es la empresa con mayor cobertura del sector con oficinas propias en todas las regiones españolas. Tiene sus oficinas centrales y domicilio social en Madrid.

ALCANCE

El alcance del sistema de información del Grupo BC contempla a los sistemas de seguridad de la información que dan soporte a los procesos de:

El servicio de:

a) formalización de operaciones hipotecarias.
b) tramitación de escrituras y documentos asimilados.
c) externalización de procesos de negocio BPO (Business Process Outsourcing), con especialización en el sector financiero.

Según la Declaración de Aplicabilidad v0. (Mortgage Formalization and Processing Delivery under SOA en vigor).

VALORES ESTRATÉGICOS

Grupo BC declara que sus valores principales son:

- Calidad de servicio
- Respeto al entorno
- Sostenibilidad y protección del medio ambiente
- Profesional
- Confianza
- Seguridad

EL TALENTO DE LAS PERSONAS COMO VALOR ESTRATÉGICO

Disponer de un equipo con la mejor formación y capacidades es un punto clave para desarrollar y mantener la fórmula de Grupo BC.

Dedicamos grandes esfuerzos en fomentar el trabajo en equipo y dotar a nuestros profesionales con las competencias claves para ofrecer un excelente servicio al cliente, apoyándonos en un gran equipo humano capaz de sacar partido a las tecnologías más punteras del mercado.

El valor de nuestro equipo de profesionales es imprescindible para desarrollar nuestro servicio y es la clave de nuestra excelencia, lo que nos hace invertir directamente en su desarrollo y en la gestión del talento

Nuestro compromiso de equipo se centra en:

- Flexibilidad y conciliación.
- Diversidad e igualdad de oportunidades.
- Identificación y gestión del talento.
- Inversión en formación continua y conocimiento.
- Fomentamos la igualdad de género.
- Fomentamos un entorno laboral seguro y saludable.

COMPROMISOS DE SEGURIDAD DE LA INFORMACIÓN DE GRUPO BC

Para ello Grupo BC adquiere los siguientes compromisos:

En **general**:

- Mejora continua del desempeño tanto de los sistemas de gestión como del resultado a obtener. Mejora de la eficacia de los sistemas.
- Actualización y cumplimiento del marco legal y de los requisitos propios y específicos que nos puedan poner tanto nuestros clientes como los proveedores y personas implicadas.
- Mantener un alto nivel de cualificación y talento para poder ser eficaces y eficientes en los procesos.
- Mantenimiento de los adecuados canales de comunicación con todas las partes interesadas, con objeto de asegurar su satisfacción con respecto al cumplimiento de sus necesidades, requisitos y expectativas

- Se adoptarán las medidas necesarias para que todo el personal de GRUPO BC sea conocedor de esta política. Difundiéndose también ésta a los proveedores y colaboradores, estando además a disposición del público a través de la página web.

En **seguridad de la información**:

Principios generales:

- Política de análisis, gestión y disminución del riesgo potencial grave. Se priorizarán las actuaciones sobre riesgos potenciales graves.
- Política de Tolerancia con las incidencias. Se investigará y sancionará aquellas actuaciones dolosas o imprudentes.
- Política de impacto reputacional mínimo. La incidencia reputacional en materia de seguridad debe tender a 0.
- Integridad y actualización de los sistemas. Mantener actualizados nuestros sistemas y asegurar la integridad de nuestra información.
- Seguridad integral. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información
- Control operacional. Controlar operacionalmente de forma eficaz las amenazas y riesgos sobre el activo y las instalaciones.
- Gestión por procesos. Organizar el sistema por medio de la implementación de los procesos de seguridad que se revisan y mejoran de forma continua
- Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.
- Cumplimiento Legal. Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información.

PRINCIPIOS Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Principios particulares y responsabilidades específicas:

- Gestionar eficientemente las incidencias que afecten a la integridad, disponibilidad y confidencialidad de la información de la empresa.
- Implantar planes de continuidad del negocio que garanticen la continuidad de las actividades de la sociedad en caso de incidencias graves o contingencias.
- Política de gestión de personas como activo de información que incluya medidas de sensibilización y/ o formación en materia de seguridad
- Gestionar los roles de los profesionales responsables del sistema de seguridad de la información para asegurar el nivel de profesionalidad necesario.
- Política de control y autorización de accesos se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.
- Política de seguridad física de las instalaciones Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Política de criterios de seguridad de la información aplicados a la gestión de proveedores y en la Adquisición de productos (sistemas y servicios)
- Protección de datos (inactivos y en tránsito/medios) se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos.
- Prevención contra la conexión a través de sistemas interconectados
- Registro de actividad
- Protección de los sistemas y de la comunicación: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

Y como compromiso con el cumplimiento de esta política firma la Dirección.

Xavier Costa Ran
CEO
GRUPO BC