

TP.100

Política de Segurança da Informação

Órgão:
Data inicial: 2006/05/25
(referência)

Versão: 1.0
Última alteração: 2006/05/25

Índice de conteúdos

1.- INTRODUÇÃO	3
2.- INFORMAÇÃO	4
3.- DEFINIÇÃO	5
4.- ALCANCE E ÂMBITO DA APLICAÇÃO	7
5.- RESPONSABILIDADE GERAL	8

1.- INTRODUÇÃO

A incorporação das novas tecnologias da informação no Grupo Banco Popular (adiante designado por Grupo) oferece novas oportunidades, novos modelos de negócio e um conjunto de vantagens competitivas associadas, permitindo melhorias de eficiência e de integração entre os diferentes sistemas.

Contudo, estas tecnologias também levam ao aparecimento de novos riscos que ameaçam um dos activos mais valiosos para os processos do negócio: **a informação.**

A complexidade associada ao uso dos sistemas de informação e o cumprimento dos requerimentos legais vigentes, aconselham a elaboração de directrizes claras e concisas que definam as normas a seguir no tratamento da informação e que complementem o estilo, práticas e costumes do nosso Grupo.

Por essa razão, a Direcção Geral do Grupo considerou necessário melhorar o seu posicionamento estratégico em matéria de segurança de sistemas, através da aprovação de uma Política de Segurança.

O objectivo desta política é a protecção eficiente da informação mediante um enfoque preventivo, detector, reactivo e dinâmico.

Assim, a presente Política de Segurança dos Sistemas de Informação constitui o pilar básico para o tratamento seguro da informação no Grupo.

2.- A INFORMAÇÃO

A informação que se produz, processa, transmite e se armazena nos sistemas informáticos do Grupo é um elemento fundamental para conseguir uma óptima gestão e controlo do seu negócio.

Para o correcto desempenho das suas funções, é indispensável que a Direcção e os empregados do Grupo possam gerir a informação em termos de:

- **Confidencialidade**, salvaguardando que apenas quem está autorizado pode aceder à informação.
- **Integridade**, assegurando que a informação e os seus métodos de recompilação e de processo são exactos e completos.
- **Disponibilidade**, garantindo que os usuários autorizados tenham acesso à informação e aos activos associados quando o solicitarem.

Deste modo, é uma obrigação legal e ética do Grupo garantir, nos mesmos termos, às instituições colaboradoras e aos organismos oficiais competentes, a informação que diz respeito aos seus clientes.

Sob estas premissas, a informação criada, processada e armazenada nos sistemas informáticos do Grupo, independentemente do seu suporte ou formato, e utilizada durante as actividades operativas e administrativas do seu negócio, considera-se um activo pertencente ao Grupo.

Inclui-se na definição anterior a informação cedida ao Grupo sob o âmbito legal estabelecido e que o Grupo considerará como activo próprio, inserido nos bens exclusivos em sua protecção.

Deve-se considerar igualmente como activos a proteger, os diferentes recursos informáticos – basicamente hardware e software – utilizados para administrar e gerir a informação pertencente ao Grupo e aqueles alugados ou licenciados pelo mesmo.

3.- DEFINIÇÃO

Estabelece-se como política de segurança que o acesso, a utilização, a custódia e a salvaguarda dos bens informáticos se realizará garantindo sempre a integridade, disponibilidade e confidencialidade da informação do Grupo, respeitando o âmbito legal vigente e cumprindo fielmente as directrizes, procedimentos e normas de acesso que se estabeleçam.

Esta política encontra-se suportada pelas premissas descritas de seguida, que devem guiar o desenvolvimento da norma que expande adequadamente as políticas para cada um dos meios, situações e ambientes existentes no Grupo:

- É política do Grupo proibir a divulgação, duplicação, modificação, destruição, uso inadequado, roubo e acesso não autorizado a informação pertencente ao Grupo ou a outras empresas e pessoas que lhe tenha sido confiada.
- Toda a informação residente nos sistemas do Grupo será protegida de acordo com a sua importância, para o que se manterá um inventário, classificação e avaliação dos activos, tendo em conta aqueles casos sensíveis ou críticos que possam ocorrer.
- A autorização de acesso a qualquer activo de informação estará determinada pela necessidade de utilização do referido activo para a realização das distintas funções operativas dentro da organização.
- O pessoal do Grupo, e qualquer outro pessoal que trabalhe sob contrato para o Grupo, deverá aceder exclusivamente à informação estritamente necessária para o desempenho das suas funções, independentemente de ter acesso físico a informação não relacionada com as referidas funções.
- Fica proibido qualquer tipo de acesso a activos do Grupo por parte de terceiros, sejam, recursos informáticos ou de informação, excepto nos casos em que se determine a necessidade, com conhecimento e autorização, mediante acordo escrito do Grupo.
- Proíbe-se às empresas subcontratadas, a prestação de qualquer serviço a terceiros utilizando os activos informáticos do Grupo, sem a autorização expressa e por escrito do mesmo.
- Estabelece-se expressamente a proibição do uso dos activos do Grupo, tanto recursos informáticos (correio electrónico, Internet, ofimática, espaço no disco, etc.) como a informação (de clientes, de terceiros, etc.), para fins distintos dos estritamente profissionais relacionados com o desempenho habitual das funções no Grupo e que não tenham sido expressamente aprovadas pela Direcção ou não tenham uma justificação evidente.
- O acesso à informação residente nos sistemas de informação do Grupo deverá realizar-se sempre através do uso de um identificador de usuário, pessoal e intransmissível, e da palavra de acesso associada (palavra-chave), que deverá permanecer sempre em segredo.

- Sob esta filosofia, fica expressamente proibida a utilização de um mesmo identificador de usuário e da sua palavra de acesso por pessoas distintas.
- É responsabilidade de cada empregado do Grupo manter em segredo a sua palavra de acesso e conservá-la por forma que não seja descoberta por terceiros, uma vez que qualquer acesso indevido com o referido identificador será da responsabilidade do seu proprietário.
- Na utilização dos serviços de Internet e correio electrónico ter-se-á em conta que associado ao usuário está o nome do Grupo ou de alguma das suas empresas. Consequentemente, ter-se-á em conta padrões de cortesia, educação e ética no exercício ou utilização dos mesmos.
- Devido aos perigos que tem a utilização de software danificado ou não autorizado, está proibida a instalação de aplicações que não se encontrem devidamente autorizadas pelo Grupo.
- A protecção dos activos do Grupo é uma tarefa que afecta todas as pessoas vinculadas directa ou indirectamente ao Grupo, sendo responsabilidade de cada um preservar a disponibilidade e integridade da informação, comunicando às áreas competentes e através das vias estabelecidas, qualquer evento ou incidência que afecte os sistemas de informação.
- O Grupo assume o compromisso de manter os seus sistemas de informação em sintonia com a norma legal vigente, especialmente com os regulamentos legais relativos ao tratamento dos dados de carácter pessoal, a informação privilegiada e a salvaguarda do segredo profissional e bancário, adoptando as medidas técnicas e organizativas necessárias.

4.- ALCANCE E ÂMBITO DA APLICAÇÃO

O âmbito da presente Política inclui todos os escritórios, unidades, áreas, departamentos, empregados e pessoal subcontratado que acedem aos sistemas de informação de todas as empresas do Grupo, assim como, as empresas externas colaboradoras.

A política é aplicável a todos os sistemas de informação das empresas do Grupo, independentemente da tecnologia que os suporte.

A política afecta todo o tipo de informação criada ou utilizada como suporte dos negócios do Grupo, independentemente do seu formato ou meio de armazenamento.

A Política constitui uma declaração da postura da Direcção do Grupo relativamente à segurança dos sistemas de informação e estabelece os objectivos, responsabilidades e comportamentos necessários para gerir os activos informáticos num meio profissional seguro.

5.- RESPONSABILIDADE GERAL

A aplicação e cumprimento da política de segurança sobre os activos informáticos é da responsabilidade de todas as empresas, escritórios, áreas e empregados do Grupo, independentemente de os referidos activos informáticos lhes terem sido atribuídos ou não, e de fazerem ou não uso destes.

Consequentemente, todos os empregados do Grupo e os terceiros subcontratados, são co-participantes da referida responsabilidade, devendo trabalhar, a partir da posição que ocupem e independentemente da responsabilidade que explicitamente lhes é atribuída, com o objectivo de concretização da Segurança adequada da informação.

Os empregados do Grupo, assim como o pessoal subcontratado ou colaboradores externos, adquirem, por sua vez, o dever de segredo, ou seja, a responsabilidade de não divulgar nenhum tipo de informação que tenham adquirido na realização do seu trabalho.

Para tal, deverão conhecer, assumir e cumprir a política, normativas e procedimentos de segurança vigentes, estando obrigados a manter o segredo profissional e a confidencialidade dos dados utilizados no meio laboral e devendo comunicar, com carácter de urgência e segundo os procedimentos estabelecidos, as possíveis incidências ou problemas de segurança que se detectem.

A direcção do Grupo adquire a responsabilidade de promover e apoiar o estabelecimento de medidas técnicas, organizativas e de controlo que garantam a integridade, disponibilidade e confidencialidade dos activos informáticos, com o fim de evitar a sua possível alteração, destruição, roubo, cópia, falsificação e outras ameaças existentes, sejam estas acidentais ou não.

O incumprimento claro das normas de segurança poderá acarretar o início das medidas disciplinares oportunas e, por sua vez, as responsabilidades legais correspondentes.