Política de Segurança da Informação

Com a finalidade de garantir a proteção da empresa de todos os pontos de vista, é necessário proteger convenientemente os nossos ativos, gerir adequadamente a segurança empresarial e maximizar a integridade, confidencialidade e disponibilidade de todos os elementos necessários para o correto funcionamento da HomeServe (clientes, informação, processos, infraestruturas, pessoas, etc.), protegendo-os contra possíveis ameaças, minimizando os riscos, maximizando o retorno dos investimentos e oportunidades e garantindo a continuidade dos processos de negócio.

No que diz respeito aos ativos da HomeServe, consideramos especialmente relevante a proteção das informações corporativas e dos elementos que as tratam. Estes ativos são, sem dúvida, essenciais para nós e para a nossa empresa e devem ser mantidos razoavelmente protegidos de quaisquer ameaças que possam colocá-los em risco. A segurança da informação deve ser assegurada sem prejuízo da proteção de outros elementos da nossa empresa, e sempre de acordo com os princípios legais, organizacionais e técnicos aplicáveis. Desta forma, cada um de nós deve conhecer e cumprir a política de segurança definida e os procedimentos, regulamentos, normas e padrões que a desenvolvem e que podem afetar a realização das nossas tarefas na empresa. Neste sentido, a direção da HomeServe estabelece um claro compromisso público de garantir os níveis de proteção adequados aos requisitos da empresa, colocando à disposição do seu pessoal todos os meios necessários para atingir este objetivo. Da mesma forma, manifesta-se o compromisso com a melhoria contínua do sistema de gestão da segurança da informação.

Com o objetivo de garantir a proteção efetiva dos recursos empresariais necessários para o correto funcionamento da empresa, tanto contra ameaças externas como internas, são definidos os princípios básicos da Política de Segurança da HomeServe, que se encontram listados abaixo:

1. Todo o pessoal da HomeServe deve conhecer, cumprir e fazer cumprir os processos ou procedimentos aplicáveis à esfera da segurança da informação, individualmente e conforme as tarefas realizadas na empresa.

2. Limitar a utilização tanto da própria informação como dos sistemas que a processam, cuja propriedade é da HomeServe, às tarefas necessárias para a correta execução do trabalho de cada pessoa dentro da empresa, não sendo, portanto, permitida a utilização de qualquer bem da empresa para benefício privado.

3. Pelo que se refere à informação, considerada como um dos principais ativos da HomeServe e cuja propriedade é de empresa, é dever de todo o pessoal manter uma estrita confidencialidade sobre a mesma e não a divulgar a terceiros, a menos que as comunicações façam parte da relação profissional.

A HomeServe pode monitorizar e investigar a utilização correta dos equipamentos, ficheiros e sistemas, perante um possível incidente de segurança.

A finalidade do referido controlo geral é verificar o cumprimento das obrigações que correspondem a cada funcionário, em relação à utilização dos meios e ferramentas informáticas, cuja propriedade é da HomeServe, visando garantir a segurança dos sistemas de informação.

O funcionário, ao aceitar o regulamento de utilização dos sistemas de informação em vigor, consente expressamente o controlo geral realizado pela empresa, que deverá ser sempre efetuado com o máximo respeito pela privacidade e dignidade de cada trabalhador.

Cada um de nós desempenha um papel fundamental para garantir a segurança da informação. Por esta razão, cabe salientar os seguintes pontos:

- Deve ser feita uma utilização responsável dos recursos da empresa, tais como correio eletrónico, equipamento de trabalho, dispositivos móveis, etc., em conformidade com o regulamento de utilização do sistema de informação.

- É especialmente importante proteger as credenciais de acesso aos sistemas de informação (nome de utilizador e palavra-passe), as quais não devem ser comunicadas a terceiros.

- As informações que tratamos são propriedade da HomeServe e, portanto, não devem ser divulgadas ou enviadas a terceiros sem autorização prévia do nosso superior hierárquico imediato.

- O pessoal do departamento de TIC ou o responsável pela segurança deve ser informado de qualquer anomalia que possa conduzir a um incidente de segurança: roubo, fugas de informação, acesso não autorizado, etc.

- É da responsabilidade de cada funcionário manter o seu posto de trabalho arrumado e impedir o acesso não autorizado à documentação em conformidade com a política relativa a postos de trabalho bem organizados e de cuidados a serem tomados com a informação visualizada pelo funcionário no ecrã.

O não cumprimento da presente política de segurança, bem como das diretrizes ou legislação aplicáveis a cada caso, conduzirá à adoção das medidas legais correspondentes conforme com o critério definido pela empresa.