Política de Segurança da Informação e Segurança Cibernética

Tagus Investimentos LTDA

31/12/2021

SEGURANÇA DA INFORMAÇÃO

A Tagus tem por principio básico a segurança e a confidencialidade das informações inerentes aos seus negócios, definindo as seguintes diretrizes como política de segurança de informação:

- Confidencialidade – Garantia de que o acesso à informação seja obtido, apenas, por pessoas autorizadas. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física;

- Integridade – Garantia de que a informação não seja adulterada falsificada ou furtada;

- Disponibilidade – Garantia de que a informação esteja disponível sempre que requisitada pelos usuários autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

As ações operacionais para atendimento das diretrizes adotadas:

- Terceirização das áreas de TI e Suporte – Será definida a contratação de uma empresa para estruturação e acompanhamento da plataforma de TI da Tagus, mediante a assinatura de um instrumento particular de contrato e aderência do contratado às politicas da Tagus.

- Contratação da plataforma de e-mails – Contratação da plataforma de e-mails Google Apps, devido à estrutura e recursos para segurança de informação que consideramos adequados para a Tagus. A plataforma permite:

- Acesso confiável aos dados 24 horas por dia, 7 dias por semana;

- Camada extra de segurança com dupla autenticação, reduzindo risco de roubo de senhas e nomes de usuário;

- e criptografia automática das sessões do navegador com SSL, sem necessidade de VPNs ou outras infraestruturas.

- Necessidade de armazenamento e backup de informações em ambiente seguro – Utilização de um storage compartilhado da marca LACIE, além da contratação do serviço de backup em nuvens (WUALA) da LACIE, armazenados de forma incremental. Os dados transferidos para o backup externo são encriptados (AES, RSA e SHA) e salvos de formas redundantes em diferentes servidores, com base na Suíça, Alemanha e França. As soluções em segurança são analisadas e validadas pelo Instituto Federal Suíço de Tecnologia de Zurique (ETH Zurich).

- Definição de limites de controle, acesso e utilização das informações - O acesso a todos os sistemas e informações da Tagus será concedido de acordo com as necessidades da função de cada usuário. O acesso somente será liberado após digitação de senha pessoal e intransferível. Os usuários assumem inteira responsabilidade pela informação acessada, se comprometendo em utiliza-la somente para fins específicos das atividades exercidas para as quais foi autorizado. O descumprimento destas regras estará sujeito a análise e penalidades por parte do Compliance da Tagus.

- Testes e Monitoramento – Todos os sistemas e ferramentas de segurança da rede da Tagus contam com acompanhamento por parte da Real Solutions em tempo real, através de acesso remoto através de senha em poder apenas do responsável indicado pela empresa e do Diretor de Compliance da Tagus, é acompanhamento físico, semanal, a fim de garantir a estabilidade da rede e a segurança das informações. Testes de segurança são realizados semestralmente em conjunto com a Real Solutions.

- Softwares piratas devem ser removidos por completo da empresa e **licenciados adequadamente**.

- A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco. As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da empresa.

- Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

- As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área sempre que esse equipamento estiver em uso ou logado com a credencial do colaborador que necessita do suporte.