-- POLÍTICA DE SEGURANÇA DA INFORMAÇÃO --

A VIACERTA é uma empresa que segue rígidos padrões de Segurança da Informação impostos pela legislação brasileira e pelas disposições do Banco Central. Uma das ações por ela realizadas é a manutenção de uma Política de Segurança da Informação que regula as atividades internas e também como os funcionários e prestadores de serviços devem tratar seus dados. Os aspectos gerais desta política são descritos neste documento.

A VIACERTA segue também segue padrões internacionais de Segurança da Informação, como as normas ISO 27002 e 27701, que definem controles corporativos para a proteção de dados. Além disso, a Política de Segurança da Informação prevê uma série de outras regulamentações internas (como Política de Acesso, Plano de Ação e de Resposta a Incidentes, Política de Backup, etc). Adicionalmente, toda a organização da Segurança da Informação visa prevenir, detectar e reduzir o risco envolvido em incidentes que atinjam o ambiente tecnológico.

Basicamente, os seguintes controles de segurança são cobertos pela Política de Segurança da Informação:

1. Organização da segurança da informação
    a. Há uma organização interna de todas as atividades relativas à Segurança da Informação. A VIACERTA mantém um cargo específico que tem como função garantir que todos os processos previstos estão sendo aplicados.

2. Segurança em recursos humanos
    a. Toda a seleção de colaboradores cumpre uma série de requisitos que visam confirmar todas as informações fornecidas pelos candidatos. Todos os funcionários assinam Termos de Confidencialidade, têm suas responsabilidades de segurança claramente definidas, passam por treinamentos periódicos e são submetidos a processos disciplinares em caso de desrespeito às suas obrigações de segurança.

3. Gestão de ativos
    a. A VIACERTA mantém inventário de todos os ativos de informação que trata. Para cada um desses ativos é mantido uma rígida categorização que prevê procedimentos específicos para o seu tratamento, envolvendo o grau de sensibilidade, criticidade e importância para o negócio.

4. Controle de acesso
    a. A instituição mantém uma política de controle de acesso que regula como seus funcionários e terceiros podem acessar os dados com segurança. Somente funcionários e terceiros contratualmente autorizados podem ter acesso aos dados, sendo todos os referidos acessos registrados e submetidos a auditoria. Igualmente, são aplicados controles para a utilização de credenciais seguras para o acesso a todas as informações.

5. Criptografia
    a. Todas as informações consideradas sensíveis - o que inclui os seus dados - são protegidas, dentre outras formas, por meio de criptografia.

6. Segurança física e do ambiente
    a. A VIACERTA mantém controles de acesso às suas instalações físicas, regulando o trânsito de pessoas em sua sede somente para situações que forem necessárias. Todos os colaboradores são orientados a manter comportamentos seguros no ambiente de trabalho e todo o ambiente conta com monitoramento via circuito interno de vídeo.

7. Segurança nas operações
    a. Todo o ambiente é organizado, inclusive quando há o uso de recursos da nuvem, para atender aos requisitos das normas de segurança. Assim, a implantação ou modificação de sistemas sempre contam com controles de segurança aplicados já nas fases de planejamento, sendo observados inclusive após sua implementação.
    b. A VIACERTA também conta com sistemas de antivírus, antimalware, firewall e detecção de intrusão, além de outras medidas técnicas de segurança. Adicionalmente, há uma política de backup para proteger as informações contra situações de perda.
    c. Todos os sistemas são monitorados ativamente, e cada acesso é registrado, sendo passível de auditoria posterior (interna e externa), cumprindo assim, inclusive, legislações como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais.

8. Segurança nas comunicações
    a. Todos os processos que realizam o trânsito de informações seguem rigorosos padrões de segurança em redes, inclusive com uso de acessos protegidos por criptografia.

9. Relacionamento com terceiros e fornecedores
    a. Sempre que um terceiro ou fornecedor de serviços precisar ter acesso aos sistemas da VIACERTA, esta atividade será antecedida pela aplicação de controles técnicos e jurídicos que preservem a segurança de toda a operação. As situações de acesso são devidamente registradas, sendo submetidas a auditoria interna e externa.
    b. As medidas de controle estabelecidas cobrem também as situações de desenvolvimento de sistemas.

10. Gestão de incidentes de segurança da informação
    a. A instituição possui uma equipe dedicada a realizar a detecção, o registro e o controle das eventuais ocorrências de incidentes de segurança. Sendo assim, incidentes que eventualmente ocorram são registrados e resolvidos, sendo as partes relevantes comunicadas. Ao mesmo tempo, são tomadas medidas para evitar que o incidente se repita, conforme as disposições do Banco Central.

11. Segurança da Informação e continuidade do negócio
    a. A VIACERTA possui um Plano de Continuidade que visa atender a uma série de situações projetadas que possam comprometer a prestação de serviços. Neste sentido, está preparada para continuar oferecendo seus serviços em situações de incidentes ou desastres que possam afetar sua infraestrutura técnica e física.

12. Conformidade
    a. A VIACERTA mantém um processo interno que visa identificar quais os requisitos legais são aplicáveis a sua estrutura e serviços. Assim, são seguidas todas as regulamentações do Banco Central, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor, além de outras regulações aplicáveis aos seus serviços prestados.
    b. Ademais, todas as partes que possuem contato com os sistemas da VIACERTA possuem contratos regulando tal relação.
    c. Por fim, todo o ambiente é auditado, a fim de verificar a aplicação da legislação e também o cumprimento de suas políticas internas de segurança.