Descrição dos procedimentos realizados

O IBRC possui uma política de segurança com base no PCI-DSS 3.2 e ISO-27002. Com base nisso, todos os dados coletados pelo IBRC independente do canal (SMS, WhatsApp, E-mail, Telefone) são considerados confidenciais e, portanto, devem ser classificados como tal. Vale ressaltar que os dados inseridos no banco de dados são criptografados, o que confere um grau de sigilo absoluto.

Outras medidas de segurança que também são adotadas pelo Instituto:

- ✓ São aplicados controles de prevenção a vazamento de dados na camada OSI, especificamente nas camadas 2 e 3;
- ✓ Todos os colaboradores que fazem manipulação dos dados oriundos dos trabalhos realizados (tanto para manutenção, quanto para sustentação do serviço) possuem um termo de confidencialidade assinado, a fim de evitar possíveis vazamento de informações;
- ✓ Todos os acessos e manutenções (logs) em bases de clientes, são devidamente registados (trilha de auditoria), sendo os logs armazenados em ambiente segregado;
- ✓ Todo desenvolvimento e homologação dos sistemas desenvolvidos pelo IBRC são realizados em ambiente de teste controlado e auditado.
- ✓ O servidor utilizado é certificado ISAE 3402 Parte II SOC 1. No escopo da certificação consta a revisão de acessos ao datacenter e, também, a política de logs de acessos;
- ✓ O IBRC não terceiriza nenhum tipo de serviço que manipula dado sigiloso (pessoal e sensível).
- ✓ Todos os servidores do Instituto são próprios e ficam em locais físicos, onde possuem o acesso controlados por meios eletrónicos.
- ✓ Todos os colaboradores são monitorados e possuem acesso apenas aos dados que são necessários para execução de suas atividades;
- ✓ Os dados pessoais e sensíveis serão removidos de forma irreversível e segura dos sistemas e backups 72h após a entrega do relatório, independentemente da massa de dados.
- ✓ As gravações ficam armazenadas em ambiente seguro, sendo o acesso possível apenas para alguns funcionários, justamente atrelado ao que foi apresentado no item anterior;
- ✓ O IBRC realiza Backups diários, os arquivos são criptografados e armazenados em local seguro.
- ✓ Os downloads de gravações são controlados e auditados periodicamente, nesse sentido, qualquer movimentação é registrada nos logs de segurança;

Por fim, afirmamos que o IBRC possui padrões e práticas de desenvolvimento seguro, com a base de comunicação *Scrum*, a fim de auxiliar o desenvolvimento a UML (Diagramas de classe, Diagrama de caso de uso), diagramas de banco de dados (Entidade relacional e Modelo relacional), baseando também o desenvolvimento no *Framework MVC Láravel*.

Este documento está em conformidade com a Política de Segurança da Informação, Política de Privacidade e Norma de Backup do Instituto IBRC.