Políticas de Segurança

Nome: Yuri Fernandes, RA: 429538

Nome: Kevin de Oliveira Bruno, RA: 627658

- Apenas o time de infra-estrutura tem acesso completo aos recursos da AWS. O restante da empresa tem acesso somente leitura.

- Todos os usuários da AWS tem que possuir ativo o MFA para acesso aos serviços.

- Os usuários possuem roles e não permissões específicas.

- Todos os usuários possuem uma politica de expiração de senha correspondente a 30 dias.

- As senhas devem possuir no mínimo 8 caracteres contendo pelo menos uma letra maiúscula e números.

- Todos os serviços e aplicações internas não devem possuir dependências com alguma vulnerabilidade independente da stack ou linguagem.

- A empresa deve possuir um time responsável (pentest) para testar possíveis vulnerabilidades em aplicações e serviços.

- Se alguma aplicação ou serviço houver qualquer vulnerabilidade o time responsável deve ser notificado e a correção dessa vulnerabilidade deve ocorrer em no máximo 7 dias.

- A empresa fornece todo o equipamento necessário ao colaborador, porém, o mesmo é responsável por manter o funcionamento do mesmo.

- Caso ocorra algum problema em qualquer equipamento fornecido, o colaborador deve entrar em contato com o setor responsável solicitando reparo.

- Todo acesso interno aos serviços e recursos da empresa devem ser por meio de uma VPN.

- Todos os computadores que a empresa fornece devem ter anti-vírus configurado de acordo com a politica da T.I.

- Todos os acessos necessários pelo colaborador de acordo com a função na qual o mesmo exerce devem ser concedidos apenas pelo time responsável pela segurança da informação da empresa.

- Todo processo de criação pelo colaborador é de propriedade da empresa, por exemplo, criação de api´s, aplicações web, ferramentas de apoio, etc...