VOLVO

Segurança Cibernética na Volvo Financial Services

Conforme determina o artigo 5º da Resolução 4.893, de 26 de Fevereiro de 2021, do Conselho Monetário Nacional, o **Banco Volvo (Brasil) S.A.** e a **Volvo Administradora de Consórcio Ltda.** (em conjunto denominadas "VFS"), divulgam, por meio deste comunicado, as linhas gerais de sua Política de Segurança Cibernética, aprovada em 02 de Agosto de 2021.

1. Introdução, Objetivos e Princípios

A Política de Segurança Cibernética visa assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informações da VFS, por meio da:

- Proteção do ambiente cibernético;
- Prevenção, detecção, resposta e investigação de incidentes;
- Execução de planos para atender situações de emergência e crises envolvendo o ambiente cibernético;
- Execução de planos de resposta a incidentes e da continuidade do negócio;
- Capacitação de seus colaboradores e terceiros, quando aplicável.

Os controles de segurança referenciados da Política de Segurança Cibernética são caracterizados pela preservação dos seguintes princípios:

- **Confidencialidade** – Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio;

- **Integridade** – Garantia de que as informações estejam exatas e completas durante o seu ciclo de vida;

- **Disponibilidade** – Garantia de que as informações e os Recursos de TIC estejam acessíveis e utilizáveis sempre que necessário por aquele autorizado.

2. Principais Diretrizes de Segurança Cibernética

As Diretrizes de Segurança Cibernética estabelecem os elementos básicos da gestão de risco cibernético, sendo:

Gestão de Acessos: A VFS controla o acesso físico e lógico aos seus ambientes, ativos e informações, baseado em critérios do mínimo conjunto necessário e estritamente necessário ao definir os acessos de seus colaboradores. Os acessos aos ambientes tecnológicos são limitados aos indivíduos registrados e autorizados e a VFS conta com ferramentas de detecção de acesso não autorizado.

Classificação da Informação: Todas as informações de propriedade ou sob a responsabilidade da **VFS** devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida, de acordo com a Diretiva de Governança da Informação do Grupo Volvo.

Ambientes Lógicos: Os sistemas de Tecnologia de Informação que suportam os acessos e informações da VFS devem ser confiáveis, íntegros, seguros e disponíveis. A VFS utiliza sistemas de proteção, ativos atualizados, contra programas maliciosos e acessos indevidos e para indicar tentativas de instrução realizada aos ambientes lógicos.

Desenvolvimento, Manutenção e Aquisição de Sistemas: O desenvolvimento externo e interno de sistemas, bem como sua aquisição, devem observar os requisitos de segurança cibernética constantes na Política de Segurança Cibernética.

Backup e Monitoramento: A VFS realiza o *back-up* de seus dados, em ambientes seguros, de forma a garantir a continuidade do negócio em caso de falhas ou incidentes. Os ambientes físicos e lógicos são monitorados para verificação da eficácia dos controles implantados.

Auditoria: A VFS realiza auditorias sobre seus processos e sistemas de TI, a fim de levantar possíveis vulnerabilidades ou oportunidades de melhoria.

Proteção de Dados Pessoais: A VFS possui controles para garantir a disponibilidade, integridade e confidencialidade dos seus dados pessoais, incluindo (a) a adoção de medidas de segurança para proteger os dados pessoais de acessos não autorizados, perda e alteração indevida; (b) armazenamento de modo seguro; (c) disponibilização a terceiros de modo seguro e contratualmente previsto, de forma a assegurar a confidencialidade das informações.

Contratos com Terceiros e Prestadores de Serviços: Todos os contratos com terceiros e prestadores de serviços devem conter cláusulas de obrigatoriedade de reporte de incidentes de Segurança Cibernética que envolvam dados que sejam de propriedade ou estejam sob a responsabilidade da VFS.

Além do exposto acima, também constam na Política de Segurança Cibernéticas diretrizes quanto à proteção de ambientes físicos, manutenção de recursos de tecnologia da informação e comunicação, análise de obsolescência de serviços e sistemas, monitoramento de ambientes físicos e lógicos, gestão de riscos e vulnerabilidades em segurança cibernética, gerenciamento de configurações de segurança da informação em seus recursos, controles de segurança cibernética em sistemas e servidores, continuidade de negócio.
Há também definido processo de revisão das diretrizes expostas na Política de Segurança Cibernética, de modo a garantir que a Política contemple os controles mais atualizados do ponto de vista tecnológico e regulatório.

3. Plano de Ação e Resposta a Incidentes

A VFS possui um Plano de Ação e Resposta a Incidentes, sendo que cada incidente de segurança cibernética passa por processo de categorização tendo em vista seu nível de criticidade, visando assegurar que quaisquer incidentes e potenciais incidentes sejam tratados de forma efetiva, permitindo o adequado registro, análise crítica, tomada de ação corretiva e escalonamento em tempo hábil. Deste modo, é possível mitigar o impacto negativo sobre os ativos de rede e sistemas de informação bem como para o cliente final que utiliza os serviços da VFS.

4. Responsabilidades

É de responsabilidade de todos os colaboradores e prestadores de serviços da **VFS** zelar pelo cumprimento da Política de Segurança Cibernética, sendo que as áreas envolvidas diretamente por garantir o cumprimento desta têm suas responsabilidades específicas definidas e estabelecidas .

A alta administração da VFS aprovou a Política de Segurança Cibernética e está comprometida com a melhoria contínua dos controles e procedimentos relacionados ao tema e com a disseminação de uma cultura de segurança cibernética.

5. Canal de Comunicação e Denuncias

Denúncias, dúvidas, sugestões ou incidentes relacionados à Segurança Cibernética da VFS, constatadas por terceiros (público em geral), devem ser comunicadas imediatamente através do email encarregado.dpo@volvo.com.