Política de Segurança de Informações

#### **Exercício 1 - Aula 5**

Davi Deosmar Batista Oliveira Miranda – RA: 823.212.282

Silas Rodrigues Nascimento – RA: 823.273.38

Política de Segurança Interna – Atividade

**1.** Do escopo deste documento

Este documento contempla as políticas de segurança a serem adotadas para a empresa WiTech, a serem adotadas tendo em vista a otimização das atividades de modo a evitar falhas de segurança e/ou exploração de vulnerabilidades por pessoas má intencionadas.

**2.** A quem se aplica?

Este documento aplica-se a todos os funcionários da WiTech, sejam eles os que trabalham via modelo remoto, ou via modelo presencial. Todos aqueles que possuírem acesso a qualquer ambiente ou sistema interno ou utilizado pela empresa estão obrigados a seguir as normas e práticas descritas neste documento.

**3.** Dos deveres da WiTech para com seus funcionários

A WiTech se compromete, através deste documento, a:

**3.1.** Armazenar os dados de seus funcionários em ambientes seguros, com tecnologias e sistemas já bem-consolidados no mercado;

**3.2.** Seguir as diretrizes e boas práticas de proteção de informações das normas da família ISO 27000, de modo que seus documentos, dados, ativos e informações digitais passem por classificação e hierarquização de informação em graus de sigilo, a saber:

- Público;

- Interno;

- Restrito;

- Secreto;

**3.3.** Punir, seja por medidas disciplinares ou demissão, ou até mesmo com medidas judiciais, todos aqueles que violarem estas políticas e lesarem quaisquer um de seus funcionários ou clientes;

**3.4.** Limitar os acessos dos usuários de seus sistemas ao mínimo privilégio possível, de modo que as permissões sejam diversas e selecionadas individualmente, e não massivas e delimitadas por cargos ou setores, de modo a garantir que certas pessoas tenham e outras não acesso a determinadas informações;

**3.5.** Realizar backups de suas bases de dados duas vezes por dia em intervalos de 12h entre cada um deles;

**3.6.** Desligar e remover os acessos aos sistemas e informações pertencentes/usados pela WiTech de cada funcionário que vir a ser desligado da mesma;

**3.7.** Monitorar erros sistêmicos via sistema de logs, de modo a ser notificada e acionada para a correção de problemas sistêmicos sempre que estes ocorrerem;

**3.8.** Fornecer dispositivos seguros e com ligação direta via VPN para os funcionários que trabalharem em regime remoto ou híbrido;

**3.9.** Utilizar softwares de segurança e de gestão de dispositivos registrados como ativos de sua empresa.

**4.** Dos deveres dos funcionários da WiTech

Os funcionários da WiTech se comprometem, mediante este termo, a:

**4.1.** Não conectar nos computadores da empresa quaisquer dispositivos e mídias físicas de armazenamento, transferência, leitura e transmissão de dados, dentre os quais, mas não limitados a: pen-drives, CDs, DVDs, HDs/SSDs externos, celulares, tablets, ou outros dispositivos não autorizados, mesmo que via Bluetooth ou conexão remota;

**4.2.** Não conectar as máquinas pertencentes à WiTech em quaisquer redes de internet que não aquelas fornecidas pela própria empresa;

**4.3.** Ao ausentar-se temporariamente durante o expediente de trabalho, realizar o bloqueio de tela de seu computador ou dispositivo móvel para prevenir o acesso e o uso do mesmo por pessoas não autorizadas;

**4.4.** Não fornecer as suas credenciais de acesso a sistemas internos e externos para nenhum outro colaborador da WiTech;

**4.5.** Não anotar senhas em mídias físicas, dentre as quais, mas não limitadas a: papéis, stickers, cadernos, agendas, entre outros;

**4.6.** Não compartilhar a terceiros nenhuma informação a si confiada que esteja em algum grau de sigilo acima de “Pública”;

**4.7.** Não enviar arquivos, informações e ativos digitais da empresa via serviços de e-mail ou mensagens digitais. Para tal, utilizar somente os sistemas internos de transferências de arquivos em VPN;

**4.8.** Não fornecer a pessoas autorizadas informações que não estejam inclusas no seu escopo de quais informações estas podem saber;

**4.9.** Comunicar a empresa em caso de qualquer detecção ou encontro de bugs, falhas sistêmicas ou vulnerabilidades nos softwares utilizados pela WiTech;

**4.10.** Não fotografar, gravar áudios, vídeos ou registrar eletronicamente quaisquer ambientes internos da empresa, em especial mas não limitando-se a: telas de computadores, documentos físicos ou digitais, entre outros.