TelePuc

Telemarketing

Cartilha de Segurança

Seja bem-vindo à Cartilha de Segurança da TelePuc! Aqui, você encontrará orientações importantes para proteger as informações e os recursos da nossa empresa. Vamos lá!

Principais orientações de segurança

Propriedade

Todas as informações geradas, acessadas, recebidas ou armazenadas pela TelePuc são propriedade exclusiva da empresa. Isso inclui nossas marcas, reputação e ativos tangíveis e intangíveis. Lembre-se sempre de utilizar os recursos de Tecnologia da Informação e Comunicação (TIC) fornecidos pela TelePuc apenas para atividades profissionais e com autorização prévia para o uso de nossas marcas em qualquer veículo de comunicação.

Classificação da Informação

- Informação Pública: Pode ser divulgada sem causar danos à empresa.
- Informação Interna: Destinada apenas aos colaboradores da TelePuc e seu acesso não autorizado pode causar impactos institucionais.
- Informação Confidencial: Exclusiva e requer tratamento especial, sua divulgação pode afetar nossa reputação e imagem, além de causar impactos financeiros, legais e normativos.

Controle de Acesso

Cada colaborador recebe uma identidade digital para acessar os recursos da TelePuc, que não deve ser compartilhada. É obrigatório portar o crachá de identificação nas dependências da empresa.

Segurança Física

Estabelecemos espaços físicos seguros para proteger áreas que criam, desenvolvem, processam ou armazenam informações críticas. É fundamental garantir a integridade e disponibilidade desses ativos.

Internet e Correio Eletrônico

O acesso à internet e o uso do correio eletrônico corporativo devem ser estritamente profissionais, respeitando as regras de direitos autorais e privacidade.

Redes Sem Fio (Wi-Fi)

O acesso à rede sem fio é restrito aos colaboradores autorizados e limitado ao perímetro da empresa. Visitantes e fornecedores poderão ter acesso à rede sem fio com prévia autorização.

Recursos de TIC

Os recursos de TIC são destinados apenas a fins profissionais e não devem ser utilizados para armazenamento de arquivos pessoais.

Dispositivos Móveis

O uso de dispositivos móveis da TelePuc não é permitido por terceiros. Em casos de roubo, perda ou furto do dispositivo móvel institucional, o colaborador deve registrar um Boletim de Ocorrência (B.O.), entregar uma cópia do documento e notificar imediatamente o gestor e a GSI.

Armazenamento de Informações

As informações devem ser armazenadas de forma segura nos locais apropriados. Informações digitais devem ser armazenadas nos servidores da rede corporativa, com controle de acesso e cópia de segurança.

Mídias Sociais

O comportamento nas mídias sociais deve ser compatível com os objetivos da empresa.

Segurança de Informação

Os colaboradores devem adotar medidas de segurança, como uso de senhas fortes e atualização de software.

Monitoramento e Incidentes de Segurança

A empresa monitora atividades para proteção do patrimônio e colabora com investigações em caso de incidentes de segurança.

Combate ao Preconceito e Discriminação

Todos os colaboradores devem participar de campanhas contra preconceito e discriminação, e cooperar em situações críticas, fornecendo informações de segurança sempre que necessário.

Código de Ética

Todos os colaboradores da TelePuc devem respeitar a PSI e o Código de Ética e Conduta da empresa, sendo responsáveis por suas ações e omissões.

Boas Práticas

Todos devem adotar boas práticas de segurança da informação, incluindo o uso de senhas fortes, proteção dos recursos de TIC, atualização de software e hardware, além de participar de treinamentos e campanhas de conscientização.

Boas Práticas

Esta PSI deve ser revisada e atualizada periodicamente para atender às necessidades e ao contexto da TelePuc, levando em consideração as mudanças na legislação, tecnologias e ambiente de negócio. As atualizações devem ser comunicadas a todos os colaboradores e demais interessados.

Seguindo essas orientações, contribuímos para manter um ambiente seguro e protegido para todos na TelePuc. Juntos, podemos garantir a confidencialidade, integridade e disponibilidade das nossas informações e recursos.