Içara, 09 de outubro de 2022.

Política de Segurança da Informação 2021- 2024

Segurança Cibernética e Proteção de Dados Pessoais:

Se você receber uma mensagem inesperada, ligação ou solicitação de informações pessoais e sentir qualquer suspeita, é crucial presumir que se trata de uma tentativa de golpe. Em caso de dúvida, recomenda-se entrar em contato diretamente com a empresa em questão, utilizando os canais de comunicação conhecidos e confiáveis.
Além disso, é fundamental nunca compartilhar informações pessoais ou confidenciais, especialmente em resposta a solicitações não solicitadas ou suspeitas. Manter suas informações privadas é essencial para proteger sua segurança e privacidade, bem como a segurança de nossa organização como um todo.
Outra prática importante é evitar clicar em links ou abrir e salvar anexos de e-mails que pareçam suspeitos ou não solicitados. Estes podem conter malware ou serem utilizados para phishing, colocando em risco seus dados e segurança online.
Lembre-se sempre: a cautela é sua melhor defesa contra golpes e ameaças cibernéticas. Ao adotar essas práticas de segurança, você contribui para proteger não apenas seus próprios dados, mas também os da nossa organização como um todo.

Assinatura Eletrônica:

A assinatura eletrônica refere-se aos dados em formato eletrônico que estão logicamente ligados a outros dados em formato eletrônico e são utilizados pelo signatário para assinar. Este processo deve obedecer aos níveis apropriados de assinatura para os seguintes atos:

Interação interna entre os órgãos e entidades da administração direta, autárquica e fundacional dos Poderes e órgãos constitucionalmente autônomos dos entes federativos.
Interação entre pessoas naturais ou pessoas jurídicas de direito privado e os órgãos e entidades da administração direta, autárquica e fundacional dos Poderes e órgãos constitucionalmente autônomos dos entes federativos. Interação entre os órgãos e entidades da administração direta, autárquica e fundacional dos Poderes e órgãos constitucionalmente autônomos dos entes federativos.

Orientações e Instruções:
Para garantir o uso adequado da assinatura eletrônica, solicitamos atenção especial aos seguintes pontos:
Segurança: Mantenha suas credenciais de assinatura eletrônicas seguras e não as compartilhe com terceiros.
Verificação: Antes de assinar qualquer documento eletrônico, verifique cuidadosamente se as informações estão corretas e se você está autorizado a assinar.
Confidencialidade: Respeite a confidencialidade das informações durante o processo de

assinatura eletrônica, garantindo que apenas as partes autorizadas tenham acesso aos documentos assinados.

Suporte técnico especializado e treinamento: Caso necessite de orientação adicional sobre o uso da assinatura eletrônica, não hesite em entrar em contato com o fornecedor do certificado, como Serpro, Certisign, Serasa Experian, Soluti, entre outros, que são credenciadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Eles fornecem suporte técnico especializado e treinamento para garantir o uso adequado e seguro da assinatura eletrônica.

Compromisso:
Ao utilizar a assinatura eletrônica, cada usuário compromete-se a seguir rigorosamente as políticas e procedimentos estabelecidos pela organização, contribuindo para a eficiência e segurança dos processos administrativos.

Proteção de Credenciais:

Manter suas senhas e credenciais de acesso seguras e confidenciais, evitando compartilhá-las ou anotá-las em locais de fácil acesso.

Uso Adequado dos Recursos de Informação:

É fundamental que utilizemos esses recursos de maneira ética e responsável, garantindo a integridade e segurança das informações. Parte desse uso responsável implica evitar o acesso a sites não autorizados e a instalação de software não aprovado. A navegação em sites não autorizados pode expor nossos sistemas a ameaças de segurança, além de comprometer a produtividade no ambiente de trabalho. Da mesma forma, a instalação de software não aprovado pode trazer riscos à segurança da informação e à estabilidade dos nossos sistemas.

Segurança Física:

É fundamental garantir a integridade e proteção desses dispositivos contra danos e acesso não autorizado. A segurança física dos nossos equipamentos não apenas protege os dados sensíveis armazenados neles, mas também contribui para a continuidade das operações e para a manutenção da produtividade. Para garantir a segurança dos dispositivos de computação, gostaria de reforçar algumas práticas essenciais:

- Mantenha os dispositivos sempre sob vigilância quando estiverem em uso e não os deixe desacompanhados em locais de acesso público.
- Evite expor os dispositivos a condições adversas, como temperaturas extremas, umidade ou impactos físicos.
- Nunca compartilhe senhas ou informações de acesso aos dispositivos com pessoas não autorizadas.

Reporte de Incidentes:

Relatar imediatamente ao secretário responsável pela área correspondente na prefeitura qualquer incidente de segurança da informação que você possa observar ou experimentar. Isso inclui situações como perda de dispositivos ou qualquer suspeita de atividades maliciosas. Ao relatar prontamente esses incidentes, garantimos uma resposta ágil e eficaz para proteger os dados sensíveis e a infraestrutura tecnológica do município contra possíveis ameaças. Nossa

colaboração ativa e conscientização são essenciais para manter a segurança e integridade dos sistemas e informações da prefeitura.
Conformidade com as Políticas: Cumprir todas as políticas e regulamentos municipais relacionados à segurança da informação, incluindo leis de proteção de dados e normas de segurança cibernética.

Lembramos a todos que a segurança da informação é responsabilidade de cada um de nós. Juntos, podemos trabalhar para identificar e mitigar os riscos de segurança, fortalecendo assim a proteção dos dados e recursos da nossa instituição.

Esta Política de Segurança da Informação é de cumprimento obrigatório para todos os funcionários e contratados da organização.

Referencias:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10543.htm acesso em 04/10/2022

validar.iti.gov.br/guia.html acesso em 04/10/2022

Atenciosamente,
Departamento de TI
Prefeitura Municipal de Içara