6.4.1. Aos Gestores das áreas cabe:
6.4.1.1. Manter postura em relação à Segurança da Informação e servir de modelo de conduta para os colaboradores sob a sua gestão;
6.4.1.2. Disseminar a POSIC para os colaboradores de suas áreas;
6.4.1.3. Comunicar de forma tempestiva, pelos meios oficiais instituídos, a revogação de acessos e recursos computacionais de colaboradores das suas áreas quando for pertinente;
6.4.1.4. Garantir a implementação de mecanismos necessários para o descarte seguro das informações;
6.4.1.5. Solicitar formalmente à GETIC os devidos acessos aos ativos de informação a serem utilizados pelo setor ou compartilhados com terceiros, usando os meios homologados pela ESP/CE;
6.4.1.6. Adaptar os processos, procedimentos e normas sob sua responsabilidade para atender à POSIC;
6.4.1.7. Observar e zelar pela aplicação das regras e legislações de proteção de dados;
6.5. USUÁRIOS INTERNOS
6.5.1. Os usuários internos têm as seguintes responsabilidades:
6.5.1.1. Cumprirem as determinações constantes nesta Política, independentemente do nível hierárquico ou função, bem como do vínculo empregatício;
6.5.1.2. Buscar orientação da GETIC quando houver dúvidas relacionadas à Segurança da Informação;
6.5.1.3. Responsabilizar-se pelo ativo de TIC e por sua adequada utilização;
6.5.1.4. Responder por toda violação de segurança praticada por si;
6.5.1.5. Utilizar os serviços e recursos somente para as necessidades autorizadas, assegurando que os recursos tecnológicos sejam utilizados apenas para fins profissionais aprovados e de interesse da Instituição;
6.5.1.6. Proteger sua senha de acesso e não compartilhar, sendo responsável por todas as ações realizadas com sua identificação;
6.5.1.7. Utilizar somente programas legalizados ou analisados tecnicamente pela GETIC, sendo expressamente, proibido o uso/instalação de software não licenciado;
6.5.1.8. Usar os serviços de forma otimizada e compartilhada, evitando desperdícios tais como utilização inadequada do tempo de rede, Internet, de impressão e espaço em disco;
6.5.1.9. Prezar pela segurança das informações confidenciais, incluindo todo e qualquer dado pessoal a que tiver acesso;
6.5.1.10. Atender à LGPD, protegendo os dados a que tiver acesso ou que venha a manuseá-los, sempre em conformidade às regras da ESP/CE;
6.5.1.11. Assumir a responsabilidade por eventuais prejuízos ou danos sofridos ou causados à ESP/CE e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.
6.5.2. É vedado aos colaboradores internos:
6.5.2.1. Realizar qualquer procedimento que envolva suporte técnico, tais como manutenção de equipamentos, instalação de software, alteração nas configurações do sistema e outras similares, sem a devida autorização da GETIC;
6.5.2.2. Acessar, via Internet, sites que comprometam a segurança e infrinjam à cultura organizacional, a legislação e as normas estabelecidas da ESP/CE;
6.5.2.3. Divulgar sua senha de acesso à rede para qualquer pessoa, pois a informação é de caráter pessoal e intransferível;
6.5.2.4. Utilizar arquivos e dados de outro colaborador interno, sem a devida autorização;
6.5.2.5. Enganar ou subverter as medidas de segurança dos sistemas e da rede de comunicação.
6.6. USUÁRIOS EXTERNOS
6.6.1. Os usuários externos têm as seguintes responsabilidades:
6.6.1.1. Cumprir os preceitos estipulados por esta POSIC, quando estiverem executando atividades no ambiente da ESP/CE;
6.6.1.2. Responder por toda atividade executada por meio de sua identificação;
6.6.1.3. Responder por toda violação de segurança praticada por si, sem prejuízo da responsabilização da contratada ou de entidade/órgão ao qual está vinculado;
6.6.1.4. Seguir as recomendações e as boas práticas de utilização dos recursos ofertados pela ESP/CE para a execução de suas atividades;
6.6.1.5. Assinar o Termo de Compromisso, formalizando a ciência e o aceite da Política de Segurança e de suas normas.
7. PRINCÍPIOS
7.1. Os equipamentos de tecnologia da informação e comunicação, os sistemas e as informações devem ser utilizados para a realização de atividades profissionais, com senso de responsabilidade e preceitos éticos comuns à sociedade e dentro da legalidade. Respeitar a privacidade dos usuários, agindo de forma ética e atendendo aos princípios da Lei Geral de Proteção de Dados.
7.2. As ações de segurança da informação da ESP/CE têm como norte as definições contidas na Política de Segurança da Informação e Comunicação dos ambientes de Tecnologia da Informação e Comunicação – TIC do Governo do Estado do Ceará, contendo os seguintes princípios orientadores:
7.3. Alinhamento Estratégico: considera o alinhamento da Política de Segurança da Informação com o Planejamento Estratégico e com os demais instrumentos de governança de TIC do Governo do Estado do Ceará;
7.4. Diversidade Organizacional: considera a diversidade das atividades da Instituição de forma a garantir a continuidade do seu negócio;
7.5. Garantia da Segurança das Informações: considera a adoção de medidas que visem garantir a confidencialidade, disponibilidade e integridade das informações da Instituição;
7.6. Propriedade da Informação: considera que toda informação produzida ou armazenada no Estado é de sua propriedade e não de seus colaboradores, exceto os casos onde a Instituição atua como custodiante da informação, devendo seu uso ser destinado, exclusivamente, a atender aos interesses da Instituição e seguindo todos os preceitos estabelecidos pela LGPD;
7.7. Alinhamento com Aspectos Legais: considera o alinhamento da Política de Segurança da Informação com as legislações vigentes e os demais regulamentos específicos aplicáveis à Administração Pública Estadual.
8. DIRETRIZES
8.1. Na POSIC foram definidas diretrizes que devem ser observadas conforme abaixo:
8.1.1. As ações relacionadas à Segurança da Informação que serão necessárias ao cumprimento desta Política devem ser consideradas na ocasião da elaboração/revisão do Planejamento Estratégico da ESP/CE;
8.1.2. Os colaboradores internos deverão realizar a entrega do Termo de Confidencialidade e Segurança da Informação, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela ESP/CE;
8.1.3. Qualquer demanda de colaboradores internos relacionados a ativos de TIC deverá ser realizada por meio do sistema de chamado definido pela ESP/CE;
8.1.4. A POSIC deverá ser disseminada de forma permanente por meio de campanhas de conscientização com o intuito de assegurar que todos os colaboradores conheçam as suas orientações;
8.1.5. Todos os usuários são responsáveis pela segurança dos ativos de informação que estejam sob sua custódia e pelo uso e guarda de suas credenciais de acesso, sendo vedada a exploração de eventuais vulnerabilidades – que, assim que identificadas, devem ser imediatamente comunicadas à DICIT/GETIC;
8.1.6. Deverá constar em todos os contratos da ESP/CE, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser cumprida por empresas fornecedoras e por todos os profissionais que desempenham suas atividades na ESP/CE, inclusive provenientes de organismos internacionais.
9. DIRETRIZES ESPECÍFICAS
9.1. As Diretrizes Específicas da POSIC são:
9.1.1. ACESSO À INTERNET
9.1.1.1. Os colaboradores devem acessar exclusivamente ferramentas, sites e aplicativos relacionados ao trabalho que desempenham;
9.1.1.2. Nos casos em que determinado colaborador necessite acessar algum conteúdo que esteja bloqueado pelos mecanismos de segurança, deverá ser aberto um chamado solicitando a liberação do acesso, onde a DICIT/GETIC fará a liberação desde que o conteúdo solicitado não proporciona riscos para a segurança da ESP/CE;
9.1.1.3. Os visitantes poderão ter acesso à internet por meio do wi-fi exclusivo para esse público ESP-VISITANTES;
9.1.1.4. Cabe à DICIT/GETIC, monitorar e bloquear automaticamente sites que contenham conteúdos contrários às legislações vigentes;
9.1.1.5. Qualquer necessidade de download de programas/softwares deve ser repassada à DICIT/GETIC, sendo registrado o pedido por meio de canal oficial definido pela ESP/CE;
9.1.2. CORREIO ELETRÔNICO
9.1.2.1. A GETIC será responsável pelo gerenciamento, adição, exclusão e adoção de medidas operacionais visando conter a propagação de e-mails suspeitos no ambiente de tecnologia da ESP/CE em conformidade com a política de segurança da informação do Estado;
9.1.2.2. A qualquer tempo, mediante detecção pelos sistemas e/ou identificação de e-mails suspeitos pela equipe de suporte responsável pelo monitoramento do sistema de correio eletrônico, a GETIC procederá com as configurações necessárias objetivando conter eventuais propagações de e-mails suspeitos na ESP/CE;
9.1.2.3. O colaborador deverá efetuar abertura de chamados técnicos no sistema de abertura de chamados da ESP/CE, quando houver necessidade de análise de e-mails suspeitos de SPAM pela GETIC;
9.1.2.4. O colaborador é responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;
9.1.2.5. O colaborador deverá evitar o envio de informações sensíveis por e-mail, a menos que seja estritamente necessário, sempre observando a LGPD;
9.1.2.6. O colaborador deverá acessar e utilizar o correio eletrônico somente para fins relacionados ao trabalho sempre respeitando as políticas de privacidade estabelecidas pela Instituição;
9.1.2.7. Antes de abrir anexos ou links enviados por remetentes desconhecidos, o colaborador deverá consultar a GETIC para análise, a fim de evitar a propagação de vírus;