1. OBJETIVOS

1.1. Tornar a Segurança da Informação o principal elemento para proteção de dados e informações armazenadas, processadas ou transmitidas através dos sistemas de tecnologia da informação (TI) utilizados pela Companhia de Saneamento de Sergipe.

1.2. Instituir diretrizes relativas à Segurança da Informação, visando assegurar a confidencialidade, integridade, disponibilidade, autenticidade e conformidade de dados, informações, documentos e conhecimentos, de propriedade ou sob a guarda da DESO.

1.3. Servir de fundamento para a definição de normas e procedimentos relacionados à segurança da informação exigida pela Companhia.

1.4. Estabelecer as responsabilidades e limites de atuação dos colaboradores e terceiros da DESO em relação à segurança da informação, reforçando a cultura interna.

2. ABRANGÊNCIA

2.1. Aplica-se a todas as pessoas que trabalham na Companhia de Saneamento de Sergipe sejam empregados, agentes públicos, terceirizados, colaboradores, consultores, auditores, estagiários e pessoas que obtiveram acesso aos Ativos de Informação. Todos esses colaboradores serão tratados nesta política como usuários.

2.2. Esta Política engloba não apenas os requisitos de segurança lógica, mas, também, os de segurança física e de pessoal nos ambientes computacionais.

3. CONCEITOS E DEFINIÇÕES

3.1. Acesso – Estabelecer conexão à Internet ou a um dispositivo para fornecer ao usuário o acesso a diversas informações, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade.

3.2. Acesso Remoto – Utilização de programas para conexão à distância entre computadores permitindo ao técnico acesso e controle ao equipamento.

3.3. Ameaça – Agentes ou condições causadoras de incidentes de segurança. Exploram as vulnerabilidades em sistemas e serviços.

3.4. Análise de Risco – Processo de identificação de ameaças e vulnerabilidades associadas a um ativo, de modo a estimar o impacto na ocorrência de um incidente.

3.5. Ativo – Qualquer bem, tangível ou intangível que tenha valor para a organização e consequentemente exige proteção.

3.6. Autenticidade – Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

3.7. Backup – Cópia de segurança, copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes.

3.8. Confidencialidade – Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado ou não credenciado.

3.9. Conformidade – Garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal.

3.10. Disponibilidade – Propriedade de que a informação esteja acessível e utilizável quando demandada por uma pessoa física ou determinado sistema, órgão ou entidade.

3.11. Gestor da Informação – Pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação. Cada informação deverá ter o seu Gestor que será indicado formalmente por titulares das áreas que desempenham atividades gerenciais e titulares dos órgãos executivos de direção, responsável pelos sistemas que acessam a informação.

3.12. Incidente de Segurança – Qualquer evento adverso, confirmado ou sob suspeita, ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a disponibilidade, a integridade, confidencialidade ou a autenticidade de qualquer ativo de informação da DESO.

3.13. Integridade – Garantia de que as informações estejam completas e fidedignas em relação à última alteração desejada durante o seu ciclo de vida, além de protegida contra alteração ou destruição não autorizada.

3.14. Log – Registro de eventos ocorridos nos sistemas computacionais. Deve conter: data e hora da atividade, identificação do usuário, do computador e dos procedimentos executados.

3.15. Monitoramento – Acompanhamento de eventuais ameaças, incidentes de segurança ou quaisquer descumprimentos às diretrizes presentes na Política ou Procedimentos de Segurança da Informação.

3.16. Risco – Combinação da probabilidade de um evento e de suas consequências, gerando incertezas nos objetivos da empresa que podem causar danos, perda de informações, perda financeira, parada de um serviço, disseminação indevida, danos a reputação, dentre outros.

3.17. Segurança da Informação – Conjunto de medidas voltadas a salvaguardar dados e informações sigilosos gerados, armazenados e processados por intermédio da informática, bem como a própria integridade dos sistemas utilizados pela companhia.

3.18. Violação – Qualquer atividade que desrespeite as diretrizes estabelecidas nesta política ou em quaisquer dos demais instrumentos regulamentares que a complementem.

3.19. Vulnerabilidade – Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser mitigados por uma ação interna de segurança da informação.

4. DIRETRIZES GERAIS

4.1. Gestão de Segurança da Informação e Comunicação (SIC)

4.1.1. Todas as ações e métodos de proteção utilizados para a SIC, devem subsidiar as atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

4.1.2. Os mecanismos de proteção devem ser planejados e os gastos na aplicação de controles devem ser compatíveis com valor do ativo protegido.

4.1.3. Os requisitos de segurança da informação e comunicações da DESO devem ser explicitamente citados em todos os termos de compromisso celebrados entre a instituição e terceiros, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, devendo também ser exigido termo de confidencialidade.

4.2. Gestão de Tratamento de Incidentes de Segurança em Rede

4.2.1. Todas as ações e métodos de proteção utilizados para a Segurança da Informação e Comunicação (SIC), devem subsidiar as atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

4.2.2. Deverão ser criados e mantidos os Plano de Gerenciamento de Incidentes e Plano de Recuperação de Desastres, formalizados e periodicamente testados, para garantir a continuidade das atividades críticas e o retorno à situação de normalidade.

4.2.3. Os Incidentes de Segurança da Informação em eventos, podem resultar em perda, dano ou acesso não autorizado às informações, devendo ser comunicados e registrados, para serem tratados de acordo com o Plano.

4.2.4. O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de SIC.

4.2.5. Todas as áreas da DESO que dependam de recursos de Tecnologia da Informação e da Comunicação deverão ser informadas sobre o Plano de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrências de eventos ou sinistros e estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

4.2.6. As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

4.3. Gestão de Riscos de Segurança da Informação e Comunicação (GRSIC)

4.3.1. A GRSIC é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação da DESO, e equilibrá-los com os custos operacionais e financeiros envolvidos.

4.3.2. As áreas responsáveis por ativos de informação deverão implementar processo contínuo de Gestão de Riscos, que será aplicado na implementação e operação da GRSIC.

4.3.3. A GRSIC deve ser implementada no âmbito da DESO visando identificar os ativos relevantes e determinar ações de gestão apropriadas, devendo ser atualizada periodicamente, no mínimo 01 (uma) vez por ano, ou oportunamente, em função de inventários de ativos, mudanças, ameaças ou vulnerabilidades. Trata-se de instrumento do programa de Gestão de Riscos que deve incluir um Plano de Continuidade de Negócios e um Plano de Gerenciamento de Incidentes.

4.4. Gestão de Continuidade de Negócios (GECON)

4.4.1. A GECON é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação da DESO e possíveis impactos nas operações de negócio, caso estas ameaças se concretizem.

4.4.2. O Plano de Continuidade de Negócio deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

4.4.3. A DESO deve desenvolver plano de contingência para seus sistemas de informação a fim de garantir a continuidade do negócio, contendo alternativas para os processos críticos e as fases de pré interrupção, interrupção e pós interrupção dos sistemas.

4.4.4. A DESO deve estabelecer procedimentos de rotina para a execução de cópias de segurança (backups) da informação, bem como para a disponibilização dos recursos de reserva, de forma a viabilizar a restauração dos sistemas em tempo hábil, controlando e registrando eventos e falhas.

4.4.5. As áreas da DESO deverão manter processo de GECON, de modo a não permitir que os negócios, baseados em Tecnologia da Informação sejam interrompidos, e também assegurar a sua retomada em tempo hábil, quando for o caso.

4.5. Gestão de Ativos de Informação

4.5.1.Toda informação utilizada pela DESO é um ativo que possui valor, devendo ser inventariados e permanentemente controlados para os seus diversos fins.

4.5.2. As medidas de proteção devem ser gerenciadas adequadamente ao longo de todo o ciclo de vida da informação, compreendendo as fases de criação, manipulação, armazenamento, transporte e descarte.

5. DIRETRIZES PARA OPERACIONALIZAÇÃO

5.1. Tratamento da Informação

5.1.1.Toda informação deve ser protegida para que não seja alterada, acessada e destruída indevidamente. A informação armazenada em meio digital deve ser protegida contra desastre físico (fogo, água, calor, fenômenos da natureza, etc.) e desastre lógico (vírus, alteração indevida de informação, etc.).

5.1.2. Os dados, as informações e os sistemas de informação da DESO devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

5.1.3. O Gestor da Informação deverá classificar o nível de confidencialidade e sigilo da informação baseando-se nos critérios predefinidos pela GTIC. A confidencialidade da informação deve ser mantida durante todo o processo de uso da informação e pode ter níveis diferentes ao longo da vida dessa informação.

5.2. Classificação da Informação

5.2.1. A classificação das informações consiste na definição de níveis de proteção que cada dado deve receber. A informação deve ser classificada de acordo com sua importância para DESO, ou seja, em termos de valor, sensibilidade e grau de criticidade em relação aos pilares de confidencialidade, integridade e disponibilidade, observadas as necessidades do negócio e a legislação em vigor, para evitar modificação ou divulgação não autorizada.

5.2.2. Todo usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pela DESO e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

5.3. Níveis de Classificação da Informação

5.3.1. Confidencial – É o nível mais alto de segurança dentro deste padrão. Indica que a informação se divulgada interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da empresa. Só deve ser acessada por usuário da DESO explicitamente indicado pelo Gestor da Informação. Para proteção desse nível de informação, jamais podem ser transmitidas via Internet sem o uso de criptografia e, quando descartadas, devem ser tomadas as providências cabíveis para que a informação seja de fato destruída, sem chance de recuperação.

5.3.2. Restrita – Informações estratégicas que se forem divulgadas serão capazes de trazer sérios danos ao negócio da DESO. Só devem estar disponíveis apenas para grupos restritos de colaboradores que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado. São ainda mais importantes que as informações confidenciais e por isso devem receber um grau de proteção ainda mais elevado.

5.3.3. Uso Interno – Informações relevantes para o funcionamento dos negócios da Companhia e devem ter sua integridade protegida, não sendo desejável que ela se torne de conhecimento público. Contudo, caso seja divulgada fora da DESO podem representar risco ou inconveniência operacional.

5.3.4. Pública – Informações corporativas que podem ser divulgadas a colaboradores, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio da DESO. Apesar de uma informação pública não precisar de nenhum tipo de proteção quanto à questão do sigilo, é conveniente que usuário nenhum tenha acesso a ela, a menos que precise de tal informação para o desempenho de suas atividades.

5.4. Monitoramento, Auditoria e Conformidade

5.4.1. É proibido o acesso, uso, guarda e encaminhamento de material não ético, discriminatório, malicioso, obsceno ou ilegal, por intermédio de quaisquer dos meios e recursos de comunicações disponibilizados pela DESO.

5.4.2. O uso dos recursos de tecnologia da informação e comunicações disponibilizados pela DESO é passível de monitoramento e auditoria, devendo a GTIC manter registros e procedimentos, como trilhas de fiscalização e outros que assegurem a conformidade por meio de rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos e rede interna da Companhia.

5.4.3. A conformidade é o conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as diretrizes, esta Política, suas Normas Complementares e os procedimentos estabelecidos para o negócio e para as atividades da DESO, bem como para evitar, detectar e tratar qualquer desvio ou não conformidade que possa ocorrer.

5.5. Controle de Acesso e Uso de Senhas

5.5.1. As regras de controle de acesso a todos os sistemas institucionais, intranet, internet, informações, dados e às instalações físicas da DESO deverão ser definidas e regulamentadas, por meio de normas internas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição.

5.5.2. A GTIC deve estabelecer critérios para a criação de senhas fortes, proteção dessas senhas, bem como a frequência de suas atualizações.

5.5.3. Deve ser realizado o registro (log) das operações de acesso, inclusão, alteração e exclusão à rede corporativa, sistemas, equipamentos de rede, Internet, banco de dados e e-mail e mantidos pelo prazo em que houver condições técnicas de sua manutenção.

5.6. Correio Eletrônico

5.6.1. O correio eletrônico é um sistema de comunicação corporativa para realização dos negócios da DESO.

5.6.2. As mensagens devem ser escritas em linguagem profissional, que não comprometa a imagem da empresa, que não vá de encontro à legislação vigente e nem ao Código de Conduta e Integridade da DESO. Fora desse contexto não devem ser enviadas.

5.6.3. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. Mensagens recebidas não coerentes com esta política devem ser eliminadas.

5.7. Acesso a Internet

5.7.1. O acesso à Internet deve ser usado para o desempenho das atividades profissionais do colaborador. Sites que não contenham informações que agreguem conhecimento profissional e para o negócio da DESO não devem ser acessados.

5.7.2. Para garantir o cumprimento dessa política caberá a GTIC a avaliação da liberação de acessos a sítios bloqueados.

5.7.3. É vedado o uso de recursos computacionais e de comunicação da DESO para disseminação de conteúdo protegido por direitos autorais, ilegais, via Torrent, FTP ou qualquer outro mecanismo de compartilhamento de arquivos.

5.7.4. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a DESO cooperará ativamente com as autoridades competentes.

5.8. Uso das redes sociais

5.8.1. A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações da DESO, deve ser regida por normas internas específicas e deve estar em consonância tanto com essa Política quanto com os objetivos estratégicos da Companhia.

5.9. Uso dos equipamentos no ambiente corporativo

5.9.1.Devem ser precedidos de autorização da GTIC, mediante a solicitação formal do gestor da área:

a) o uso de microcomputadores portáteis pertencentes a DESO, bem como a retirada de equipamentos de sua propriedade para fora de suas dependências;

b) o uso, nas dependências da DESO de equipamentos de informática que não sejam de responsabilidade desta;

c) no caso de utilização de equipamentos portáteis da DESO no desenvolvimento das atividades fora das dependências da companhia, o usuário fica responsável pela guarda, conservação e utilização do respectivo equipamento, além de assegurar que as informações da empresa não sejam comprometidas.

5.9.2. Dispositivos móveis:

a) no caso de furto ou roubo de um dispositivo móvel fornecido pela DESO, é de responsabilidade do usuário, registrar um boletim de ocorrência (BO) junto a autoridade policial e notificar imediatamente seu gestor direto e a GTIC.

b) a DESO, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

5.10. Acesso Remoto

5.10.1. A GTIC pode realizar acesso remoto a um computador para realização de suporte técnico.

5.10.2. O acesso remoto realizado por terceiros deve ser avaliado pela GTIC visando identificar as necessidades técnicas e o que o terceiro terá acesso, podendo ser negado caso sejam identificados riscos.

5.11. Conscientização, sensibilização e treinamento dos usuários

5.11.1. A DESO deverá promover capacitação, reciclagem e o aperfeiçoamento de todos os usuários da companhia, por meio de programas de divulgação,

sensibilização, conscientização e treinamento em segurança da informação e comunicações, com o propósito de criar uma cultura de segurança dentro da companhia.

5.11.2. Para uma efetiva proteção das informações, as Unidades Organizacionais deverão manter um plano contínuo de capacitação de recursos humanos em segurança da informação, de modo a promover maior consciência da responsabilidade individual do colaborador.

6. COMPETÊNCIAS E RESPONSABILIDADES

6.1. Conselho de Administração – aprovar a Política de Segurança da Informação e suas alterações.

6.2. Diretoria Executiva

6.2.1. Dar suporte à promoção da cultura de segurança da informação e comunicação na companhia;

6.2.2. Aprovar os documentos normativos derivados, que permitam a implantação desta política;

6.2.3. Aprovar programa orçamentário específico para as ações de SIC, conforme proposto pela GTIC.

6.3. Gerência de Tecnologia da Informação e Comunicação (GTIC)

6.3.1. Assessorar a Diretoria na promoção e disseminação de segurança da informação e comunicações;

6.3.2. Definir o escopo e os limites da Segurança da Informação e Comunicações na DESO;

6.3.3. Propor investimentos e definir a ordem de prioridade de execução dos projetos e aplicação dos recursos necessários ao cumprimento desta Política, monitorando sua aplicação;

6.3.4. Propor normas e procedimentos relativos à Segurança da Informação e Comunicações;

6.3.5. Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações;

6.3.6. Avaliar, revisar e analisar criticamente esta Política e suas normas complementares, visando à aderência aos objetivos estratégicos da DESO e às legislações vigentes;

6.3.7. Acolher e analisar as demandas quanto à Segurança da Informação e Comunicações;

6.3.8. Acompanhar os Coordenadores responsáveis pelo Tratamento e Resposta a Incidentes em Redes Computacionais da DESO.

6.4. Gestor responsável para Tratamento e Resposta a Incidentes em Redes

6.4.1. Observar os eventos de segurança com o objetivo de determinar tendências e padrões de atividades de invasores, com vistas a adotar e recomendar estratégias de prevenção adequadas. Coletar indicadores estatísticos;

6.4.2. Pesquisar informações sobre novas ameaças a redes computacionais, novas soluções para conter as ameaças e informar às áreas responsáveis;

6.4.3. Pesquisar informações referentes a novas atualizações dos softwares instalados na rede;

6.4.4. Comunicar incidentes de segurança a unidades competentes para fins estatísticos.

6.4.5. Examinar todas as informações disponíveis sobre um incidente, incluindo artefatos, evidências e logs relacionadas ao evento;

6.4.6. Identificar o escopo do incidente, sua extensão, natureza e quais os impactos causados;

6.4.7. Emitir documentos com recomendações para o tratamento correto dos incidentes após análise e investigação.

6.5. Gestor da Informação

6.5.1. Indicar a classificação da informação sob sua competência, de modo a estabelecer como essas informações podem ser acessadas e administradas, garantindo a segurança da acessibilidade e disponibilidade destas.

6.5.2. Autorizar os colaboradores acesso ou decesso às informações sob sua competência;

6.5.3. Aplicar medidas que visem garantir que o pessoal sob sua supervisão proteja as informações a que tem acesso;

6.5.4. Comunicar à GTIC, através de relatório circunstanciado, todo incidente de SIC que ocorra no âmbito de suas atividades;

6.5.5. Auxiliar na investigação de incidentes de segurança em ativos sob sua responsabilidade;

6.5.6. Participar das decisões relacionadas a qualquer violação de segurança dos ativos sob sua responsabilidade;

6.5.7. Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

6.5.8. Comunicar formalmente ao gestor da GTIC para medidas cabíveis, o remanejamento, transferência, cessão ou demissão de usuários subordinados;

6.6. Usuários (empregados, agentes públicos, terceirizados, colaboradores, consultores, auditores, estagiários e pessoas que obtiveram acesso aos Ativos de Informação)

6.6.1.Cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta política;

6.6.2. Manter a segurança dos ativos e processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações;

6.6.3. Comunicar ao gestor da unidade, os incidentes que afetam a segurança dos ativos de informação e da comunicação ou quaisquer riscos que venha a tomar conhecimento;

6.6.4. Participar de programas de treinamento online ou presencial acerca da segurança da informação, sempre que ofertados;

6.6.5. Não utilizar serviços de e-mail gratuitos para atividades institucionais, visto que tais serviços não possuem garantia de autenticidade, disponibilidade e confidencialidade das informações;

6.6.6. Utilizar sua conta de e-mail corporativo apenas para fins institucionais e de forma a não cometer qualquer ato que possa prejudicar o trabalho, a imagem de terceiros ou da própria DESO;

6.6.7. Acessar a Internet apenas para navegação em sítios cujo conteúdo esteja adequado aos dispositivos legais, às determinações da DESO e às suas atribuições institucionais.

6.7. Prestadores de Serviços

6.7.1 A Gerência de Tecnologia da Informação e Comunicação (GTIC) da DESO, deve estabelecer procedimentos para manter a segurança dos recursos de processamento de informação e ativos de informações organizacionais acessados por prestadores de serviços.

6.7.2. Os procedimentos e controles para acesso às informações devem ser acordados e definidos por meio de cláusula de confidencialidade constante dos contratos firmados com as empresas prestadoras de serviços.

6.7.3. Os contratos de prestação de serviços que envolvam manuseio, produção ou armazenamento de informações críticas ou sensíveis fora do ambiente da DESO devem conter cláusula que obrigue a manutenção desses recursos acondicionados em ambientes seguros e com controles de acesso adequados de acordo com normas técnicas estabelecidas pela DESO.

6.7.4. Os prestadores de serviço devem estar em conformidade com a Política de Segurança da Informação e com o Termo de Responsabilidade e Sigilo, que deve ser por eles aceito e assinado, a fim de que sejam feitas as liberações de acesso aos sistemas de informação da DESO.

7. DISPOSIÇÕES FINAIS

7.1. A divulgação das regras e orientações de segurança da informação, aplicadas aos usuários, deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, seminários de conscientização e quaisquer outros meios, com vistas à criação de uma cultura de segurança da informação no âmbito da DESO.

7.2. A segurança e proteção da informação é uma responsabilidade continua de cada usuário da Companhia em relação às informações que acessa e gerencia.

7.3. O descumprimento ou violação, pelo usuário, das regras previstas nesta Política poderá resultar na aplicação das sanções previstas em normas internas e legislação em vigor.

7.4. O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar à DESO, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

7.5. Os casos omissos a esta Política de Segurança da Informação serão analisados e decididos pela GTIC.

7.6. Esta Política, Normas e Procedimentos que dela se originaram deverão ser atualizadas com periodicidade mínima anual ou quando mudanças significativas, que afetem a base de avaliação de risco original, ocorrerem.

DATA DA REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO	RESOLUÇÃO DO CONSELHO DE APROVAÇÃO
17/05/2022	RCA Nº 02 / 2022