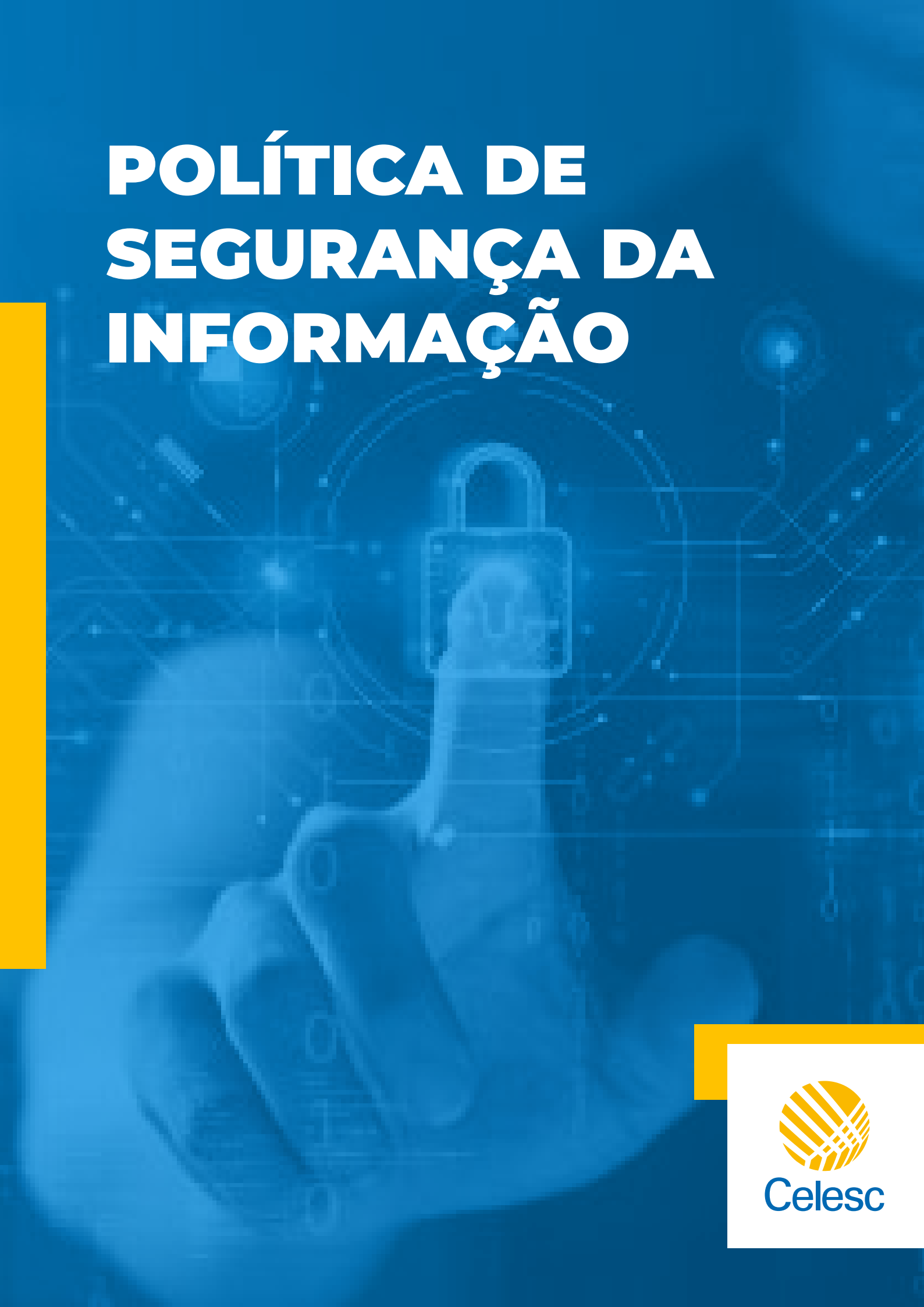
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



Celesc

Índice

1. FINALIDADE

Consentir que a informação corporativa é um bem essencial para suas atividades e, para resguardar a qualidade e garantia dos serviços prestados a seus clientes consumidores, parceiros e investidores, estabelecer sua Política de Segurança da Informação como parte integrante do seu sistema de gestão corporativa, alinhada às boas práticas e normas internacionalmente aceitas, garantindo níveis adequados de proteção às informações da organização ou sob sua responsabilidade e dispondo sobre a capacidade para prevenir, detectar, responder e reduzir as vulnerabilidades a incidentes cibernéticos. Outras diretrizes, procedimentos, normas e recomendações darão suporte a esta Política através de documentos complementares e procedimentos operacionais internos.

2. ÂMBITO DE APLICAÇÃO

Aplica-se a qualquer indivíduo ou entidade que solicite, acesse, detenha ou compartilhe dados corporativos sob a responsabilidade da Celesc.

3. ASPECTOS LEGAIS

a. ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação;

b. ABNT NBR ISO/IEC 27002 – Código de Prática de Segurança da Informação;

c. Decreto-Lei 2.840/1940 – Código Penal;

d. Lei 9.609/1998 – Lei do Software;

e. Lei 10.406/2002 – Código Civil;

f. Lei 12.527/2011 – Lei de Acesso à Informação;

g. Lei 12.965/2014 – Marco Civil da Internet;

h. Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;

i. Código de Conduta Ética da Celesc;

j. Política de Consequência da Celesc;

k. Política de Privacidade da Celesc;

l. NIST – National Institute of Standards and Technology;

m. Resolução Normativa ANEEL 964, de 14 de dezembro de 2021;

n. Rotina Operacional RO-CB.BR.01 da ONS – Operador Nacional do Sistema Elétrico;

o. Decreto 11.856, de 26 de dezembro de 2023 – Política Nacional de Cibersegurança;

p. Decreto 9.573, de 22 de novembro de 2018 – Política Nacional de Segurança de Infraestruturas Críticas;

q. Decreto 10.778, de 16 de julho de 2021 – Rede Federal de Gestão de Incidentes Cibernético.

4. CONCEITOS BÁSICOS

4.1. Informação

Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, que possam constituir referências a acontecimentos, fatos ou fenômenos..

4.2 Segurança da Informação

É a preservação das propriedades da confidencialidade, integridade e disponibilidade das informações, sendo uma constante manutenção, envolvendo tecnologia, conscientização e cultura organizacional.

4.3 Software

É o conjunto de componentes lógicos que controla o funcionamento de um computador, também chamado de programa de computador.

4.4 Engenharia Social

Engenharia Social é um termo utilizado para representar a habilidade de conseguir acesso a informações confidenciais ou a áreas restritas. Em geral, engenheiros sociais se aproveitam de relações de confiança, bem como da falta de conscientização de empregados com relação à Segurança da Informação para obter informações confidenciais da empresa.

4.5 Vulnerabilidade

Qualquer fator que possa contribuir para gerar invasões, roubos de dados ou acessos não autorizados a recursos.

4.6 Patches de Atualização

São as pequenas atualizações lançadas pelo fornecedor de software para a correção de pontos de segurança ou qualquer outro item dentro do sistema que vá garantir o melhor funcionamento.

4.7 Tecnologia Operacional

A Tecnologia de Operação (TO) refere-se ao conjunto de hardware e software dedicados ao monitoramento e controle de dispositivos físicos e processos dentro de uma organização. Ela é comumente associada a sistemas de controle industrial, como SCADA (Supervisory Control and Data Acquisition), sistemas de controle distribuído (DCS) e outros sistemas de automação utilizados em ambientes de produção e infraestrutura crítica.

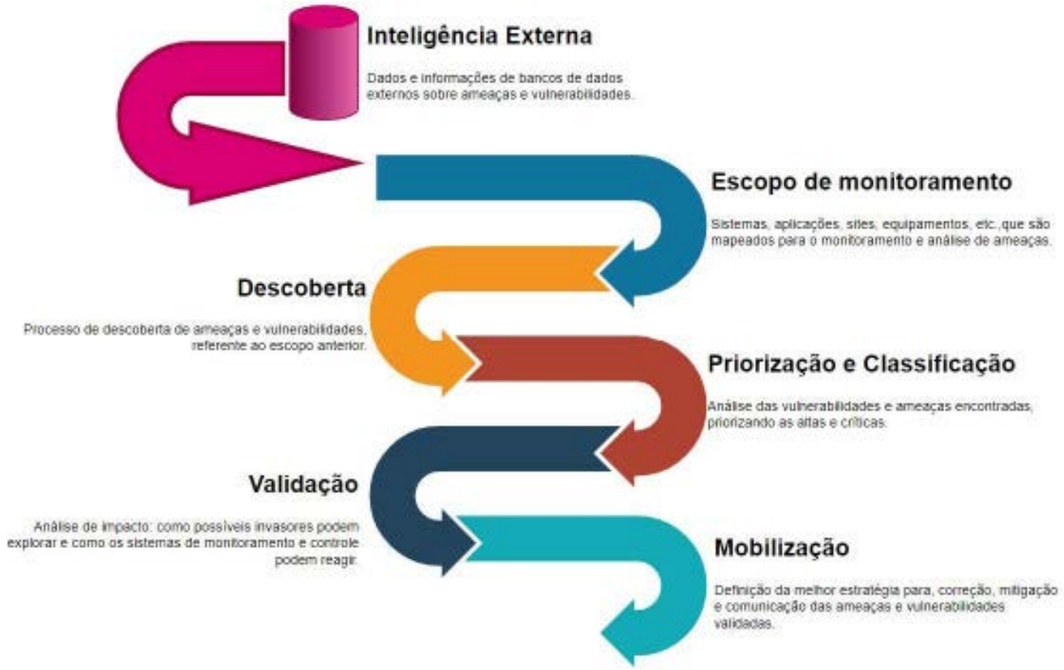
4.8 Tecnologia Operacional

Refere-se ao conjunto de técnicas, ferramentas, processos e sistemas usados para criar, processar, armazenar, transmitir e gerenciar informações.

5. PROCEDIMENTOS GERAIS

A Divisão de Segurança da Informação – DVSG utiliza um modelo de maturidade e capacidade, juntamente com frameworks de apoio. Ambos os componentes são integrados na política de segurança da informação para garantir uma abordagem proativa na gestão da segurança. O modelo de maturidade orienta a evolução das capacidades, enquanto o framework de controles fornece ferramentas práticas para a implementação das medidas de segurança necessárias.

A política foi desenvolvida com base no monitoramento ativo de riscos e ameaças. Sendo assim, todo acesso corporativo, seja de sistemas, empregados ou terceirizados, deve ser monitorado pelo Centro de Operações em Segurança Cibernética – SOC.



5.1 Propriedade

Toda informação corporativa é de propriedade da Celesc, sendo um bem que possui valor cujas propriedades devem ser protegidas, cuidadas e gerenciadas adequadamente. Cumprir a Política e as Normas de Segurança da Informação fazem parte desse zelo pelas informações e devem servir como subsídio na utilização dos recursos disponibilizados.

Considerando que os recursos computacionais e informações colocadas à disposição dos empregados devam ser utilizados apenas para fins profissionais e/ou para finalidades explicitamente aprovadas para o exercício das funções e relacionadas aos objetivos da empresa, a Celesc reserva-se o direito de, sempre que julgar necessário e observando-se os preceitos legais, monitorar, inspecionar ou auditar as informações que se encontram armazenadas em tais equipamentos e instalações ou trafeguem pela rede da empresa.

Todos os empregados que possuam informações sob sua gestão estão sujeitos às regras referentes ao sigilo profissional e devem garantir proteção adequada a essas informações, sendo que somente ocorrerá a concessão ou privilégio de acesso às informações corporativas quando devidamente autorizados por instância superior (Gestores e/ou Departamento de Gestão de Pessoas – DPGP).

5.2 Classificação da Informação

As informações devem ser avaliadas e classificadas quanto ao seu valor estratégico para o processo, à criticidade, aos requisitos legais e regulatórios, bem como às obrigações contratuais.

É responsabilidade do proprietário da informação classificá-la de acordo com o seu respectivo grau de sigilo no ato da elaboração. A responsabilização, os procedimentos detalhados de classificação, assim como a reclassificação, descarte e gestão das informações, estão detalhados em instrução normativa interna.

5.3 Gestão de Vulnerabilidades

A Divisão de Segurança da Informação da Celesc, em busca constante de mitigar possíveis incidentes cibernéticos, realiza rotineiramente atividades preventivas contra vulnerabilidades, detectando e sugerindo correções de acordo com o nível de criticidade da vulnerabilidade em relação ao nível de criticidade dos recursos tecnológicos envolvendo a Celesc.

As vulnerabilidades são classificadas de acordo com os seguintes níveis: críticas, altas, médias e baixas e são priorizadas de acordo a respectiva classificação.

5.4 Plano de Resposta a Incidentes de Segurança da Informação

A Celesc possui em seus procedimentos internos plano para resposta a incidentes de segurança da informação, sob responsabilidade da Divisão de Segurança da Informação.

Ele visa garantir que a organização esteja preparada para identificar, responder e mitigar qualquer incidente que possa comprometer a integridade, confidencialidade ou disponibilidade dos dados.

O plano é revisado periodicamente para assegurar a sua eficácia e promover a melhoria contínua.

5.5 Controles de Acesso e Gerenciamento de Identidade

Todos devem seguir as normas específicas de segurança da informação para controle de acesso, estabelecidas nas instruções normativas internas. Essas normas têm o objetivo de minimizar a exposição da empresa a danos que possam resultar do uso não autorizado dos recursos da empresa.

As normativas estabelecem padrões e diretrizes mínimas para o controle de acesso e gerenciamento de identidades nos sistemas da infraestrutura de TI e TO da Celesc, independentemente da origem da conexão.

5.6 Segurança para Endpoints

A Todo software que necessite ser instalado para realização de atividade vinculada ao exercício das funções na Celesc deve ser homologado pelo Departamento de Tecnologia da Informação – DPTI.

É terminantemente proibida a utilização de software não licenciado. O Departamento de Tecnologia da Informação poderá desinstalar qualquer software sem licença ou ilegal, sem prejuízo do disposto na Lei 9.609/1998 (Lei do Software).

Softwares de avaliação devem ser excluídos ou licenciados até o final do período de avaliação gratuita permitido.

5.7 Armazenamento de Arquivos Corporativos em Nuvem

O armazenamento de arquivos corporativos em locais externos à infraestrutura de TI da Celesc, como anexos de e-mails não corporativos, Google Drive, Dropbox e outros serviços de uso pessoal, é proibido.

A Celesc disponibiliza recursos oficiais, padronizados pelo Departamento de Tecnologia da Informação, para o armazenamento corporativo de arquivos na nuvem. Esses recursos oferecem controle, classificação e camadas adicionais de segurança, além de atenderem aos requisitos dos órgãos regulatórios e outras normativas.

5.8 Diretrizes de Segurança para Utilização da Internet

O acesso à internet fornecido pela Celesc deve ser utilizado exclusivamente para consulta, pesquisa, suporte, serviços e outros objetivos específicos da empresa. Esse acesso deve ser realizado através de softwares homologados pelo Departamento de Tecnologia da Informação e em conformidade com as instruções normativas internas.

Voltar ao Índice

5.9 Gerenciamento de Atualizações e Patches

A Celesc faz a gestão de atualizações e aplicação de patches, sempre seguindo as recomendações dos fabricantes.

As Divisões de Segurança da Informação e de Infraestrutura de TI são as responsáveis por aplicar patches e atualizações no ambiente da Celesc, assim como criar e aplicar os procedimentos operacionais, podendo delegar a atividade desde que orientada por um analista das divisões mencionadas.

Todo software ou hardware instalado no ambiente da Celesc deve respeitar as versões mais seguras aplicáveis disponíveis, fornecidas pelos fabricantes ou desenvolvedores legais do software ou hardware, evitando-se assim vulnerabilidades e ameaças.

Qualquer software ou hardware que indicar falha de segurança crítica ou ameaça ao ambiente da empresa, proveniente de falta de atualização e detectada pela Divisão de Segurança da Informação, poderá ser isolado ou retirado de operação, até que a falha seja corrigida ou mitigada.

5.10 Desenvolvimento Seguro de Sistemas

O desenvolvimento de sistemas deve ser conduzido em conformidade com a segregação dos ambientes de desenvolvimento, homologação e produção. Deve ser utilizado o Guia para Desenvolvimento Seguro, conforme disponibilizado pela Divisão de Segurança da Informação, garantindo assim a integridade e a segurança dos processos.

5.11 Mecanismos de Rastreabilidade da Informação

A Celesc implementa medidas técnicas para possibilitar o rastreamento de informações, sempre que aplicável tecnicamente e viável, a fim de possibilitar análise e investigação de incidentes de segurança da informação. Todo ativo que tenha poder de comunicação, seja ele um sistema ou equipamento, deve ter possibilidade de coleta de registros de informações, eventos ou logs. A Divisão de Segurança da Informação pode a qualquer momento solicitar acesso para conferência destes registros.

5.12 Mecanismos de Disseminação da Cultura em Segurança Cibernética

A Divisão de Segurança da Informação é responsável pelo espaço criado na intranet da empresa para disseminação de informações, campanhas e dados sobre Segurança da Informação.

Na criação de campanhas de conscientização, o alinhamento é feito com a área de comunicação da Celesc, a fim de potencializar o alcance para todos os empregados e demais interessados.

A Divisão de Segurança da Informação também planeja e executa simulações de ataques, como phishing em grupos de alvos específicos, a fim de estudar medidas de mitigação e entender melhor as ameaças cibernéticas na Celesc. Nos casos em que o ataque é consolidado, o empregado poderá ser direcionado a uma sessão básica de capacitação sobre o tipo de ataque sofrido.

5.13 Segurança Cibernética na Operação do Sistema Elétrico

Para mitigar o risco cibernético e aprimorar a proteção do ambiente operacional (TO) da Celesc, a segurança cibernética nas operações da empresa deve seguir o Programa de Segurança Cibernética na Operação do Sistema Elétrico. A Divisão de Segurança da Informação é responsável por estabelecer as diretrizes do programa, que é implementado em duas frentes: Técnica e Governança. O objetivo principal é proteger a infraestrutura crítica do sistema elétrico e evitar danos à rede elétrica e aos consumidores.

5.14 Acesso a Dados Corporativos por Agentes Externos

5.14.1 Definição de Agente Externo

Um agente externo é qualquer indivíduo ou entidade que solicite acesso a dados corporativos sob a responsabilidade da Celesc.

5.14.2 Procedimentos para Solicitação de Acesso

Quando a solicitação envolver o envio ou acesso a dados massivos, a área receptora da solicitação deve encaminhá-la à Diretoria Colegiada para aprovação, acompanhada do parecer do Departamento de Compliance e Riscos – DPCR e do Termo de Cooperação.
Em caso de aprovação, a solicitação será enviada ao Departamento de Tecnologia da Informação para análise técnica e verificação do cumprimento dos requisitos de segurança da informação.

5.14.3 Critérios de Segurança

Todos os acessos externos devem seguir os critérios técnicos de segurança da informação estabelecidos pelo Departamento de Tecnologia da Informação, conforme descrito em instrução normativa interna.

Os agentes devem respeitar as Políticas de Privacidade da Celesc https://privacidade.celesc.com.br/politica-privacidade/.

5.14.4 Responsabilidades do Agente Externo

O agente externo é responsável por implementar mecanismos de segurança adequados para o manuseio dos dados solicitados.

O agente externo deve assinar um acordo de confidencialidade e não divulgação dos dados.

5.15 Atribuições e Responsabilidades

5.15.1 Todas as pessoas abrangidas pela presente Política devem:

a) assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Celesc, ou seja, somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas;

b) buscar orientação visando a não utilização de software não licenciado ou a qualquer outro conteúdo que venha a infringir os aspectos de propriedade intelectual;

c) não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

d) utilizar os dados dos sistemas informatizados de acesso restrito e manter a necessária cautela no momento da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

e) não se ausentar da estação de trabalho sem bloquear ou encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros;

f) não revelar a senha da credencial de acesso aos sistemas da Celesc a ninguém e tomar o máximo de cuidado para que esta permaneça somente em conhecimento pessoal;

g) alterar a senha, sempre que obrigatório ou que tenha suposição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

h) buscar apoio junto ao Departamento de Tecnologia da Informação para a identificação de situações que possam significar uma falha de segurança;

i) guardar a privacidade e o sigilo das informações de que venha a ter conhecimento em razão do exercício de suas atividades, bem como das informações disponibilizadas pela Celesc. A guarda da privacidade e do sigilo das informações não diz respeito somente a terceiros, mas também em relação aos empregados da própria entidade que não tenham a real necessidade de conhecimento das informações;

j) utilizar as informações disponibilizadas pela Celesc somente nas atividades a que aquelas dizem respeito e nas quais compete ao empregado exercer, não podendo transferi-las a terceiros, seja a título oneroso ou gratuito, estando ciente de que suas ações ou consultas serão monitoradas, acompanhadas e eventualmente auditadas;

k) guardar o sigilo e a privacidade das informações de credenciais de acesso (identificação de usuário e senha), dados estes considerados pessoais e intransferíveis, para acesso aos sistemas e informações

disponibilizadas pela empresa, sendo o proprietário da credencial de acesso responsável pelo uso indevido desta;

l) informar imediatamente ao Departamento de Tecnologia da Informação acerca de qualquer violação das regras de proteção das informações eletrônicas ou não, por parte dele ou de quaisquer outras pessoas, inclusive nos casos de violação não intencional ou culposa, que possam comprometer a integridade, a confidencialidade e a disponibilidade da informação;

m) estar ciente de que constituem infração de concorrência desleal a divulgação e/ou utilização desautorizadas de informações e/ou segredos de negócios, relativos às informações de que venha a ter conhecimento em razão de serviços prestados à Celesc;

n) agir de acordo com os princípios da Lei Geral de Proteção de Dados, quando a atividade desempenhada lidar com dados pessoais protegidos pela lei, assegurando-se de guardar toda informação pessoal e a tratando com a devida importância e responsabilidade exigida pela LGPD, de acordo com a Política de Privacidade da Celesc.

5.15.2 Departamento de Tecnologia da Informação – DPTI

Departamento de Tecnologia da Informação – DPTI

O DPTI deve:

a) analisar os incidentes e casos de violação das regras definidas pelas políticas de segurança, encaminhando aos gestores responsáveis, quando cabível;

b) analisar incidentes e alertas de segurança da informação, a fim de buscar formas de correção ou mitigação dos riscos cibernéticos;

c) realizar a gestão de acesso dos empregados aos sistemas de informação da Celesc;

d) propor iniciativas de melhorias relacionadas à segurança da informação, principalmente quando estas estiverem alinhadas com as estratégias corporativas de negócio da empresa;

e) realizar o planejamento e a alocação de recursos financeiros, humanos e de tecnologia para o desenvolvimento de projetos de segurança da informação;

f) divulgar periodicamente informações de conscientização, visando elevar a compreensão dos riscos de segurança, bem como as medidas adequadas para evitar ou reduzi-los;

g) caso haja necessidade funcional de informar assuntos confidenciais de sua função a outros empregados, essa informação não poderá ultrapassar o estritamente necessário para a execução da tarefa a estes destinada;

h) garantir, junto com o Departamento Jurídico – DPJR e de Compliance e Riscos – DPCR, que a coleta, o armazenamento e o uso de dados pessoais sigam as regras e procedimentos estabelecidos pela Lei Geral de Proteção de Dados.

5.15.3 Gestores

Compete aos gestores:

a) cumprir e fazer cumprir a Política de Segurança da Informação e as normas complementares de Segurança da Informação;
b) responsabilizar-se pelas ações envolvendo os temas de Segurança da Informação propostos pelo Departamento de Tecnologia da Informação.

5.15.4 Comitê de Segurança da Informação

As atribuições do Comitê são:

a) analisar o impacto das políticas internas de segurança no âmbito da Celesc;

b) analisar o impacto de regulamentações sobre segurança da informação voltadas ao setor elétrico;

c) assessorar sobre o plano de resposta a incidentes de segurança da informação;

d) deliberar sobre itens específicos da Política de Segurança da Informação;

e) propor normas internas relativas à segurança da informação;

f) assessorar a implementação das ações de segurança da informação;

g) colaborar e propor ações sobre conscientização e capacitação em segurança da informação;

h) assessorar a Divisão de Segurança da Informação nas análises de risco de segurança, pertinentes aos indicadores da Celesc.

6. DISPOSIÇÕES FINAIS

A infração à Política de Segurança da Informação poderá acarretar ao infrator, e para aqueles que colaborarem com ele, sanções administrativas previstas na Política de Consequência, sem prejuízo das sanções legais previstas na legislação nacional.

Outras diretrizes, procedimentos, normas e recomendações darão suporte a esta Política através de documentos complementares e procedimentos operacionais.

7. Anexos

Não há.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Abril de 2025

Diagramação

Partners Comunicação