Eletrobras

Política da Segurança da Informação e Comunicações da Eletrobras Distribuição Alagoas

Versão 1.0

05/03/2013

Sumário

Eletrobras
Distribuição Alagoas

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

1. Objetivo

Proteger a informação custodiada, gerada, adquirida, processada, transmitida, armazenada e descartada por qualquer ativo, de diversos tipos de ameaça, garantindo a continuidade, a integridade, a confiabilidade e a disponibilidade da informação inerentes às atividades da Eletrobras Distribuição Alagoas

2. Conceitos

Ameaça: Representa o tipo de ação capaz de efetivamente prejudicar os ativos da empresa e, consequentemente, pôr em risco a integridade, confidencialidade e disponibilidade das informações.

Ativo: Qualquer bem, tangível ou intangível, que tenha valor para a Empresa.

Confidencialidade: Garantia de que a informação não esteja disponível, ou seja, não seja revelada a indivíduos, entidades ou processo de trabalho não autorizados.

Disponibilidade: Garantia de que os usuários autorizados tenham acesso às informações e aos ativos correspondentes, sempre que necessário.

Gestor da informação: Empregado da Eletrobras Distribuição Alagoasresponsável pela administração e classificação das informações geridas nos processos de trabalho sob sua responsabilidade.

Incidente: Evento não desejado, que pode resultar em danos à propriedade, perda ou extravio de informações.

Integridade: Salvaguarda da exatidão e inteireza da informação e dos métodos de processamento.

Recurso de tecnologia da informação: Recursos que processam, armazenam e/ou transmitem informações, tais como aplicativos, sistemas, estações de trabalho, *notebooks*, servidores de rede, equipamentos de conectividade e infraestrutura.

TIC: Tecnologia da Informação e Telecomunicações.

Usuário: Empregados, estagiários, aprendiz, contratados, prestadores de serviços, parceiros e fornecedores que utilizam, de forma autorizada, as informações custodiadas ou de propriedade da Eletrobras Distribuição Alagoas

Vulnerabilidade: Representa o nível de exposição a ameaças num contexto específico.

3. Referências

Decreto nº. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Decreto nº. 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
Instrução Normativa Nº 01 do GSIPR - Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008.
Norma Complementar Nº 03/IN01 DSIC/GSIPR - Departamento de Segurança da Informação e Comunicações, 10 de junho de 2009.
Norma NBR ISO/IEC 27001 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos, 28 de agosto de 2006.
Norma NBR ISO/IEC 27002 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação, 10 de setembro de 2007.
COBIT 4.1 – Control Objectives for Information and related Technology. ISACA, ITGI, 2007.
ANSI-ISA 99 - Manufacturing and Control Systems Security.

4. Diretrizes

- **Conformidade**

Devem garantir que todos os requisitos de segurança legais e/ou instituídos pela empresa estejam sendo cumpridos, assegurando o nível de segurança desejado

- **Propriedade**

Devem garantir que toda informação custodiada, gerada, adquirida, processada, transmitida, armazenada e descartada na empresa seja considerada de sua propriedade e utilizada por todos no estrito interesse da empresa.

Devem garantir que o uso das informações adquiridas de terceiros sigam um processo formal, que envolva desde a documentação até a cessão de direito por parte de seu proprietário.

Devem garantir que a cessão das informações custodiadas ou de propriedade da empresa sigam um processo formal, que envolva desde a documentação até sua cessão de direito à terceiros.

- **Proteção**

Devem assegurar que todos tenham o dever de proteger as informações custodiadas ou de propriedade da empresa contra o uso indevido, garantindo sua integridade, confidencialidade e disponibilidade, bem como informar oportuna e fielmente os incidentes nesse sentido, evitando ou mitigando perdas para a empresa.

- **Classificação da Informação**

Devem garantir que as informações custodiadas ou de propriedade da empresa sejam identificadas por seus gestores da informação, a quem compete classificá-las quanto à confidencialidade, integridade e disponibilidade de acordo com sua relevância e criticidade para os processos da empresa.

Devem garantir que a classificação da informação seja respeitada durante todo o ciclo de vida de uma informação, ou seja, sua criação, manutenção, armazenamento, transporte e descarte.

- **Controle de Acesso**

Devem assegurar que as informações e os recursos da empresa somente sejam acessados por usuários devidamente autorizados e controlados por ferramentas de segurança, respeitando a classificação atribuída a cada informação.

Devem garantir que os processos de trabalho sejam distribuídos de forma que nenhuma pessoa tenha o controle de todas as etapas, sem a intervenção de outra que seja capaz de efetuar uma verificação.

- **Utilização de Informações e dos Recursos de Tecnologia da Informação**

Devem assegurar que as informações e/ou os recursos colocados à disposição dos usuários sejam utilizados apenas para as finalidades lícitas, éticas e administrativamente aprovadas, e que suas configurações não sejam alteradas sem aprovação prévia.

Devem assegurar que as informações custodiadas ou de propriedade da empresa sejam descartadas respeitando o nível de classificação atribuída a elas.

- **Monitoramento**

Devem assegurar que o monitoramento, controle e registro dos acessos às informações e uso dos recursos e serviços sejam realizados por meio de parâmetros gerais para a identificação de possíveis causas de quebras de segurança da informação.

Devem assegurar que somente usuários autorizados e/ou recursos de TIC, previamente homologados, pelo DGT sejam conectados à rede interna.

Devem garantir a realização de verificações periódicas de forma a avaliar o cumprimento ou necessidade de adequação a estas diretrizes e demais regulamentações de segurança da informação em vigor.

Devem garantir o monitoramento do tráfego de informações efetuado por meio dos recursos de tecnologia da informação, rastreando eventos críticos e evidenciando possíveis incidentes, dando ampla e geral divulgação dessa atividade e da possibilidade de uso desse recurso em caso de incidentes, de acordo com os critérios estabelecidos, bem como, realizar testes frequentes de segurança para verificar a efetividade dos controles e da aplicação destas diretrizes além de identificação proativa de vulnerabilidades de segurança da informação.

- **Conscientização**

Devem assegurar que todos estejam cientes das ameaças e das preocupações que possam intervir na segurança das informações, e que sejam orientados a cumprir estas diretrizes, por meio da existência de um programa de capacitação e de disseminação da cultura em segurança da informação na empresa.

Devem garantir que estas diretrizes e normas correlatas sejam divulgadas a todos de forma permanente, sendo de responsabilidade de cada um o seu cumprimento, possibilitando a empresa fomentar os princípios de segurança da informação e comunicações.

- **Continuidade da Operação**

Devem garantir a continuidade das operações da empresa baseadas nos recursos disponíveis, de forma a reduzir a um período aceitável qualquer eventual interrupção, através da combinação de ações de prevenção e recuperação.

- **Prevenção e Resposta a Incidentes**

Devem assegurar que medidas preventivas sejam tomadas com o objetivo de diminuir o risco de incidentes de segurança na empresa, mantendo para tanto, uma área responsável, competente e preparada para dar resposta a incidentes e tratamento aos casos deste tipo.

- **Comunicação de Incidentes**

Devem assegurar que seja estabelecido um canal de comunicação para atender e orientar nos casos de incidentes de segurança a informação na empresa e garantir que o conhecimento de qualquer desvio ou falha na segurança das informações seja imediatamente comunicado à área responsável, a qual deverá tomar as providências cabíveis.

- **Sigilo Profissional**

Devem assegurar que os usuários estejam sujeitos às regras referentes ao sigilo profissional, devendo garantir adequada proteção, considerando cláusulas contratuais e termos de confidencialidade e sigilo, Regimento de Pessoal e outros documentos regulatórios da empresa.

- **Ambiente de Produção**

Devem assegurar que o ambiente de produção dos sistemas e processos que suportam a TIC da empresa possa garantir recursos de tecnologia da informação confiáveis, íntegros e oportunos, a quem deles necessite para execução de suas atividades profissionais.

- **Desenvolvimento de Sistemas**

Devem assegurar que o desenvolvimento interno e/ou externo de sistemas, assim como os sistemas e produtos adquiridos no mercado, seja provido dos requisitos de segurança necessários para garantir informações confiáveis, íntegras e oportunas.

- **Análise dos Ativos**

Devem assegurar a periodicidade da análise dos processos e recursos de forma que estejam devidamente inventariados e com seus proprietários identificados e cientes, bem como que as vulnerabilidades e ameaças de segurança estejam identificadas.

- **Documentação**

Devem assegurar que os sistemas e processos da empresa tenham documentação adequada e suficiente para garantir seu entendimento, sua continuidade e recuperação em situações de contingência.

- **Terceirização ou Prestação de Serviços**

Devem manter a segurança da informação quanto às regras definidas nesta política, quando a responsabilidade pelos processos ou mesmo parte deles, for terceirizada ou fizer parte da prestação de serviços, provendo auditorias periódicas, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusulas de responsabilidade e confidencialidade previamente estabelecidas.

Devem assegurar que quando da contratação de serviços, os contratos ou documentos afins possuam cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta política.

- **Publicidade**

Devem assegurar que as diretrizes, normas de segurança da informação e documentos correlatos sejam amplamente divulgadas, com o objetivo de torná-los um instrumento acessível e disponível para todos que interagirem com a empresa e que, direta ou indiretamente sejam afetados.

- **Medidas Disciplinares**

Devem assegurar quando do não cumprimento de algum dos princípios expressos nesta política pode resultar na adoção de medidas disciplinares, de caráter educativo, sem prejuízo da adoção de medidas administrativas e/ou judiciais, quando se tratar, ademais, de infrações contratuais e/ou legais, do Regimento de Pessoal e outros documentos regulatórios da empresa, além da legislação vigente.

- **Privacidade**

Devem Garantir a privacidade dos dados pessoais dos usuários em conformidade com a legislação vigente, regulamentos e normas que regem as atividades da empresa.

5. RESPONSABILIDADES

Diretoria Executiva:

Aprovar o conteúdo desta política, seus documentos associados e respectivas alterações, bem como propiciar os meios necessários para a Gestão da Segurança da Informação.

Comitê de Segurança da Informação e Comunicações – Comitê de SIC:

Coordenar, orientar e avaliar as atividades relativas à segurança da informação na empresa.

Departamento de Tecnologia da Informação e Telecomunicações – DGT:

Monitorar a aplicação das diretrizes desta política.
Revisar e alterar esta política, sempre que se fizer necessário.
Elaborar as normas e procedimentos associados a esta política.
Submeter esta política e demais documentos para aprovação do Comitê de SIC.
Implementar os controles necessários para aplicação destas diretrizes.
Coordenar as ações de planejamento, gerenciar e apoiar os projetos de TIC consonantes com o Planejamento Estratégico, voltados para as demandas internas da empresa, contemplando aquisições, entrega, suporte de bens e serviços e monitoração dos ambientes de TIC, garantindo alta disponibilidade, *performance,* eficiência e interatividade entre as unidades de negócios da Empresa.

Usuários dos Recursos de Tecnologia da Informação:

Obedecer às diretrizes desta política, mantendo a constante vigilância sobre as informações custodiadas ou de propriedade da empresa.
Informar ao DGT qualquer necessidade de alteração nesta política.

6. Disposições Gerais

- Toda e qualquer excepcionalidade ou caso omisso nesta política deve ser analisado pelo Departamento de Tecnologia da Informação e Telecomunicações.

- As eventuais necessidades de alterações nesta Política, com o objetivo de otimização dos processos ou sua atualização face às novas legislações sobre o assunto, devem ser submetidas à Diretoria Executiva, com as devidas justificativas.

- O não cumprimento dos termos desta Política sujeita o empregado infrator às penalidades previstas na Norma DG-GP-01/N-001 Deveres dos empregados proibições e penalidades e legislação em vigor.

- O não cumprimento dos termos desta Política sujeita o estagiário, aprendiz, contratado, prestadores de serviços, parceiros e fornecedores infrator às penalidades previstas nas legislações cabíveis.

- Esta política será complementada por normas e procedimentos inter-relacionados, que serão considerados partes integrantes deste documento e serão detalhados e divulgados em documentos específicos, como, por exemplo, uso de recursos de tecnologia da informação, do correio eletrônico, da rede interna, da Internet, de senhas, entre outros.