Eletrobras

POLÍTICA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E TELECOMUNICAÇÕES

Versão 2.0
21/10/2015

Sumário

1 Objetivo

Fornecer diretrizes, critérios e suporte administrativo à implementação e preservação da segurança da informação e comunicações, garantindo certos critérios de controle, quais sejam: da eficiência, da efetividade, da competitividade empresarial, da confidencialidade, da integridade, da disponibilidade, da autenticidade e da conformidade; assim como, dos Ativos de Tecnologia de Informação e Telecomunicação (ATICs) que as sustentam, tudo isso de forma alinhada com o Planejamento Estratégico Empresarial.

Estabelecer por meio de sua Diretoria Executiva as orientações estratégicas de segurança aplicáveis quanto ao uso das Informações e dos ATICs da Eletrobras, definindo os controles de segurança aplicáveis de acordo com os níveis dos riscos envolvidos.

2 Conceitos

- **Ameaça**

Causa potencial de incidente indesejado que pode resultar em danos e perdas para a empresa.

- **Ativo**

Qualquer recurso que tenha valor para a empresa.

- **Ativos de Tecnologia de Informação e Telecomunicação (ATICs)**

Todo elemento que processa, guarda ou transmite dados e informações.

- **Colaborador**

Empregado, requisitado, contratado para exercer cargo em comissão, estagiário, terceirizado, conveniado, credenciado, fornecedor, cliente, menor aprendiz, ou qualquer outra pessoa natural ou jurídica que venha a relacionar-se, direta ou indiretamente, com a empresa.

- **Evento de Segurança da Informação**

Ocorrência identificada de um estado de sistema, serviço ou rede, indicando possível violação à Política de Segurança em Tecnologia da Informação e Telecomunicações,

falha de controles ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

- **Internet**

Rede mundial de computadores, na qual o usuário pode, a partir de um computador, caso tenha acesso e autorização, obter informação de qualquer outro computador que também esteja conectado à rede.

- **Risco**

Combinação da probabilidade de um evento e de suas consequências que podem causar danos a uma organização, perda de informações, perda financeira, parada de um serviço, dentre outros.

- **Tecnologia da Informação e Telecomunicações (TICs)**

Área do conhecimento que compreende o estudo e a implementação de tecnologia usada para processamento, armazenamento e transmissão de dados, envolvendo tanto *software* quanto *hardware*, bem como redes de computadores e telecomunicações.

- **Violação**

Qualquer atividade que desrespeite as diretrizes estabelecidas na Política ou em quaisquer dos demais instrumentos regulamentares que as complementem.

3 Referências

- BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**. Brasília, DF, 13 de jun. 2000. p.2. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>.

- BRASIL. Decreto Nº 4.553, de 27 de dezembro de 2002. 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. **Diário Oficial da União**. Brasília, DF, 16 de nov.2012. p.1. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7845.htm>.

- BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5°, no inciso II do § 3° do art. 37 e no § 2° do art. 216 da Constituição Federal; altera a Lei n° 8.112, de 11 de dezembro de 1990; revoga a Lei n° 11.111, de 5 de maio de 2005, e dispositivos da Lei n° 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**. Brasília, DF, 18 de nov. 2011. p.1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>.

- BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 01/IN01/DSIC/GSIPR : Atividade de Normatização. **Diário Oficial da União**. Brasília, DF, 15 de out. 2008. Seção 1. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_1_normatizacao.pdf>.

- BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 02/IN01/DSIC/GSIPR: Metodologia de Gestão de Segurança da Informação e Comunicações. **Diário Oficial da União**. Brasília, DF, 14 de out. 2008. Seção 1. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_2_metodologia.pdf>.

- BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 03/IN01/DSIC/GSIPR: Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. **Diário Oficial da União**. Brasília, DF, 03 de jul. 2009. Seção 1. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf>.

- BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo: Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**. Brasília, DF, 25 de fev. 2013. Seção 1. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>.

- BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo: Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**. Brasília, DF, 17 de ago. 2009. Seção 1. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>.

- BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 07/IN01/DSIC/GSIPR: Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. **Diário Oficial da União**. Brasília, DF, 16 de julho 2014. Seção 1. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_7_controle_acesso.pdf>.

- BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 08/IN01/DSIC/GSIPR: Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**. Brasília, DF, 24 de ago. 2010. Seção 1. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_8_gestao_etir.pdf>.

- BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 09/IN01/DSIC/GSIPR: Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta. **Diário Oficial da União**. Brasília, DF, 16 de julho 2014. Seção 1. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_9_criptografia.pdf>.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:** Tecnologia da Informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: 08 de dez. de 2013.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da Informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro: 08 de dez. de 2013.

- ISACA. ITGI. **COBIT 4.1**: Control Objectives for Information and related Technology. 2007.

4 Princípios

- Preservar e proteger a informação gerada, adquirida, processada, transmitida e armazenada por qualquer ATIC de propriedade e/ou responsabilidade da empresa, dos diversos tipos de ameaça.

- Formalizar e consolidar os principais aspectos de estruturação e estabelecimento das Diretrizes de Segurança que compõem a Política Integrada de TIC.

- Prevenir e reduzir os impactos gerados por incidentes de segurança, assegurando a efetividade, a eficiência, a confidencialidade, a integridade, a disponibilidade, a autenticidade e a conformidade da informação da empresa.

- Estabelecer as diretrizes estratégicas e responsabilidades relativas às questões relacionadas à segurança da informação, possibilitando a criação de normas, procedimentos e instruções de trabalho de segurança.

- Assegurar que o Gestor de Segurança da Informação e Telecomunicação possa realizar o gerenciamento da estrutura de Segurança dos ATICs, para alcance dos objetivos estabelecidos, definindo, analisando e priorizando as ações necessárias.

- Estabelecer um Plano Anual de Capacitação voltado à manutenção das habilidades além do aperfeiçoamento dos colaboradores da Eletrobras na gestão de tecnologia e segurança da informação.

5 Diretrizes

- **Abrangência**

A Política de Segurança em Tecnologia da Informação e Telecomunicações deve ser aplicada a todos os usuários internos e externos que venham a ter acesso, de forma direta ou indiretamente, às informações e os ATICs da Eletrobras.

- **Publicidade**

Deve ser assegurado pela Eletrobras que esta política e suas normas complementares estejam amplamente divulgadas aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com a organização e que, direta ou indiretamente, são impactados.

- **Interpretação**

Esta Política e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, tudo que não estiver expressamente permitido só poderá ser realizado após prévia autorização, devendo ser levado em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

- **Disponibilidade**

A empresa deve garantir que a informação e/ou recurso esteja oportunamente acessível sempre que necessário e mediante a devida autorização para seu acesso e/ou uso.

- **Integridade**

A empresa deve garantir a completa informação, de forma que seja correta e verdadeira e não esteja corrompida, sem perda das suas características originais.

- **Confidencialidade**

A empresa deve garantir que a informação seja acessível apenas ao(s) colaborador(es) pertinentes.

- **Conformidade**

A empresa deve assegurar que a informação seja aderente a leis, regulamentos e obrigações contratuais aos quais os processos de negócios estão sujeitos, isto é, a critérios de negócios impostos externamente e a políticas internas.

- **Autenticidade**

A empresa deve garantir que a informação seja fidedigna e capaz de identificar sua autoria.

- **Temporalidade**

A empresa deve garantir que a informação com valor comprobatório para fins de auditorias, legais e judiciais, seja preservada na forma e pelo prazo mínimo prescrito na legislação ou regulamentação vigente.

- **Propriedade**

As informações geradas, acessadas, manuseadas, armazenadas ou descartadas por um colaborador no exercício de suas atividades, bem como os ATICs disponibilizados, são de propriedade e/ou direito de uso exclusivo da empresa e devem ser empregados unicamente para fins profissionais, limitados às atribuições do cargo e/ou função desempenhadas pelo colaborador, que deve cumpri-las dentro do padrão de conduta ética estabelecida pela empresa e em observância à sua obrigação legal de sigilo profissional.

- **Utilização dos Recursos**

A empresa deve assegurar que seus ATICs sejam utilizados apenas para fins profissionais, de modo lícito, ético e aprovado formalmente.

- **Mobilidade e Redes Sociais**

Os ATICs fornecidos pela empresa podem ser utilizados para atualização de seus colaboradores, bem como para estimular a cooperação entre eles. Desse modo, qualquer uso de ATIC que permita maior mobilidade, bem como a participação em ambientes de relacionamento, como Redes Sociais, deve estar diretamente relacionado ao trabalho, no âmbito das atribuições do colaborador. O desrespeito a essa condicionante, ocasionando dano, por ação ou omissão do colaborador, poderá implicar em responsabilidade pessoal, mediante apuração de responsabilidade, através da instauração de processo administrativo.

- **Controle de Acesso**

A empresa deve controlar o acesso aos seus ATICs e, desse modo, garantir que cada colaborador possua uma credencial de uso individual, intransferível e de conhecimento exclusivo. A empresa deve, ainda, orientar seus colaboradores sobre a sua

responsabilidade quanto ao uso e sigilo, além de coibir o compartilhamento de credenciais, sob qualquer hipótese.

- **Ciclo de vida da Informação**

A empresa deve prover ferramentas que permitam ao colaborador aplicar as melhores práticas de segurança no ciclo de vida da informação, que vai deste a sua criação, passando pelo registro e classificação, acesso, manuseio, reprodução, transmissão, guarda até o seu descarte.

- **Classificação da Informação**

A empresa deve assegurar que seus colaboradores respeitem controles compatíveis com a classificação da informação, através da implementação de ferramentas e processos. A Eletrobras deve, ainda, orientar aos seus colaboradores que, em caso de dúvida, as informações devem ser rotuladas no mínimo como de uso interno, ou seja, não passível de revelação, publicação ou compartilhamento externo, exceto em caso de determinação legal, judicial ou administrativa para a divulgação da informação.

- **Propriedade Intelectual**

A empresa é a detentora, também, de todos os direitos patrimoniais relativos às suas marcas e nomes comerciais e, portanto, deve proibir o uso não autorizado de suas logomarcas, identidade visual e quaisquer outros sinais distintivos, atuais e futuros, em qualquer forma ou mídia, inclusive na Internet.

- **Sigilo**

A empresa deve orientar aos seus colaboradores para não revelar, publicar ou divulgar quaisquer informações de propriedade ou sob a responsabilidade da empresa sem prévia autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que tais informações sejam públicas ou haja determinação legal, judicial ou administrativa de divulgação.

- **Terceirização ou Prestação de Serviços**

Todos os relacionamentos e contratações em que haja o compartilhamento de informações da empresa e/ou a concessão de qualquer tipo de acesso aos seus ambientes e ATICs, devem ser precedidos por Termos de Confidencialidade e cláusulas que tratem especificamente da Segurança da Informação e Telecomunicação. A empresa

deve prover auditorias periódicas que visem certificar o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

- **Análise dos ATICs**

A empresa deve analisar, em intervalos regulares, seus processos e ATICs, assegurando que esses estejam devidamente inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

- **Ambientes de ATIC**

Deve ser assegurado pela empresa que os ambientes dos sistemas e processos que suportam os ATICS sejam confiáveis, íntegros e estejam disponíveis a quem deles necessitem para execução de suas atividades profissionais.

- **Segurança Física e do Ambiente**

A empresa deve estabelecer perímetros de segurança para proteger as áreas que contenham ATICs, bem como inserir controles e registros apropriados para assegurar o acesso somente aos colaboradores autorizados e ATICs homologados.

- **Desenvolvimento de Sistemas**

Deve ser atestado pela empresa que o desenvolvimento interno e/ou externo de sistemas, assim como os sistemas e produtos adquiridos no mercado, sejam providos dos requisitos de segurança necessários para garantir informações confiáveis, íntegras e oportunas.

- **Documentação**

A empresa deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvem ATICs.

- **Monitoramento**

A empresa deve comunicar aos seus colaboradores sobre o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, seus ATICs, além de seus ambientes, físicos e lógicos, para verificação da eficácia dos controles implantados, proteção de seu patrimônio e reputação, rastreando eventos críticos e evidenciando possíveis incidentes.

- **Inspeção**

Sempre que se constate risco, a empresa pode inspecionar fisicamente quaisquer recursos tipificados como ATICs que porventura interajam com seus ambientes, lógicos ou físicos e/ou suas informações, incluindo os ATICs de propriedade de terceiros.

- **Equipe de Resposta a Incidentes**

A empresa deve adotar medidas preventivas para diminuir os riscos de incidentes de segurança da informação com a criação e manutenção de uma Equipe de Resposta a Incidentes em Segurança da Informação, que pode ter composição fixa ou variável, e seja competente e preparada para dar resposta a incidentes e tratamento aos casos desse tipo.

- **Comunicação de Incidentes**

A empresa deve possuir um canal de comunicação junto aos seus colaboradores para reportar imediatamente os casos de incidentes de segurança da informação, podendo fazer de modo formal ou com uso do recurso de denúncia anônima.

- **Continuidade do Negócio**

As diretrizes desta Política devem orientar os processos e o planejamento estratégico da empresa na disponibilidade e continuidade das operações dos ATICs, visando mitigar os riscos de interrupção causados por incidentes de segurança, através da combinação de ações de prevenção e recuperação, mantendo os níveis de serviço acordados.

- **Violações e Penalidades**

As violações de segurança da informação devem ser avaliadas e, se constatado um incidente, devem ser aplicadas as sanções administrativas previstas em cláusulas contratuais, normativos internos e outros documentos regulatórios da empresa, além da legislação vigente, mediante apuração de responsabilidade através da instauração de processo administrativo.

- **Tentativa de Burla**

A mera tentativa de burla às diretrizes e controles estabelecidos pela empresa, quando constatada, deve ser tratada como uma violação.

- **Conformidade**

A empresa deve possuir e manter um programa de revisão/atualização, no mínimo bienal, dessa política e dos demais instrumentos regulamentares subordinados a ela,

visando à garantia de que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente e alinhados com a política de negócios da empresa.

- **Alterações**

As alterações e atualizações desta política e de suas normas complementares devem ser comunicadas pela empresa aos seus colaboradores.

- **Capacitação**

A empresa deve possuir um Plano Anual de Conscientização em Segurança da Informação visando à capacitação e disseminação da cultura de Segurança da Informação junto aos seus colaboradores em relação ao uso ético, seguro e legal das novas tecnologias e ferramentas de trabalho, bem como das informações e recursos disponibilizados.

6 Responsabilidades

- A **Diretoria Executiva da Eletrobras-DEE** deve aprovar a Política de Segurança em Tecnologia da Informação e Telecomunicações.

- O **Comitê de Segurança de TIC** deve analisar e avaliar as ocorrências de violações e demais eventos negativos relativos à Segurança da Informação e Telecomunicação na empresa, acionando a área responsável por TIC ou outras áreas impactadas/responsáveis quando necessário; assessorar na implantação das ações de segurança da informação e comunicações na Empresa; propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com a legislação ou regulamentação vigente.

- A **Área responsável por TIC na Eletrobras** deve atuar como coordenadora/gestora da implementação e manutenção desta Política.

- O **Gestor responsável pela Segurança da Informação e Telecomunicação** deve identificar e analisar os riscos de segurança ligados aos ATICs para avaliar a necessidade de melhorias nos controles existentes; acompanhar as investigações e as avaliações dos danos decorrentes da quebra de segurança; propor instrumentos regulamentares complementares específicos para a proteção dos ATICs; apoiar as áreas

na definição de controles adequados de Segurança da Informação e Telecomunicação; promover, de forma eficaz a divulgação e a conscientização sobre segurança de informação e telecomunicação na empresa; analisar criticamente e de forma periódica esta Política e os demais instrumentos regulamentares relacionados à mesma, revisando e avaliando se o Sistema de Gestão da Segurança da Informação e Telecomunicação continua alinhado com os requisitos de negócio da empresa; atuar pró-ativamente em relação às ameaças e aos incidentes reportando-os ao Comitê de Segurança de TIC; manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, para o trato de assuntos relativos à segurança da informação e comunicações.

- A **Equipe de Resposta a Incidentes** deve avaliar, monitorar e gerir os eventos de segurança da informação, sejam eles detectados ou notificados, com a formalização de procedimentos para assegurar respostas rápidas, efetivas e ordenadas, acionando a área responsável impactada quando necessário.

- Aos **Chefes das Unidades Organizacionais** cabe gerenciar o cumprimento desta Política por parte de seus colaboradores, mapear, implantar e testar os controles de Segurança da Informação e Telecomunicação específicos dos processos de seu Departamento, especialmente daquelas atividades que não sejam dependentes de ATICs.

- Os **Colaboradores** devem cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, através do uso de forma responsável, profissional, ética e legal os ATICs, respeitando os direitos e as permissões de uso concedidas pela empresa.

7 Disposições Gerais

- O presente documento deve ser lido e considerado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes, adotados pela empresa. Além disso, esta política deve ser desdobrada em outros documentos normativos específicos, sempre alinhados às diretrizes e princípios aqui estabelecidos.

- Esta política foi aprovada por meio da Resolução 577/2015 de 21/10/2015.