



Eletrobras

**POLÍTICA DE SEGURANÇA
DA INFORMAÇÃO DAS
EMPRESAS ELETROBRAS**

Versão 2.0
28/09/2018



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DAS EMPRESAS ELETROBRAS

Sumário

1	Objetivo.....	3
2	Conceitos.....	3
3	Referências	4
4	Princípios	4
5	Diretrizes	4
6	Responsabilidades.....	7
7	Disposições Gerais	8
8	Anexo.....	8

1 Objetivo

Orientar estrategicamente as questões relacionadas à segurança da informação, definindo diretrizes para armazenamento, custódia, processamento, transmissão e descarte de informação no ambiente convencional ou de tecnologia das empresas Eletrobras.

2 Conceitos

▪ Ativo

Qualquer recurso que tenha valor para as empresas Eletrobras.

▪ Colaborador

Diretores, conselheiros, empregados, contratados, prestadores de serviço, estagiários e jovens aprendizes que atuem nas empresas Eletrobras.

▪ Gestor de informação

Titulares das áreas que desempenham atividades gerenciais e titulares dos órgãos executivos de direção superior, conforme norma específica.

▪ Incerteza

Estado, mesmo que parcial, da deficiência de informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade. A incerteza pode se transformar em ameaça ou em oportunidade para a empresa.

▪ Informação

Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

▪ 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.

▪ Segurança da Informação

Proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e sistemas.

▪ Violação

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

3 Referências

- ABNT ISO GUIA 73:2009 – Gestão de riscos.
- ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.
- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.
- Decreto nº. 3.505/2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Instrução Normativa IN 01/2008 GSI – Disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
- 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.
- Código de Ética e de Conduta das Empresas Eletrobras.

4 Princípios

- **DISPONIBILIDADE:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
- **INTEGRIDADE:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
- **CONFIDENCIALIDADE:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
- **AUTENTICIDADE:** propriedade que garante que a autoria e a origem da informação sejam sempre identificáveis.

5 Diretrizes

5.1 Público alvo

- Esta política deve ser aplicada a todos os colaboradores das empresas Eletrobras que venham a ter acesso, de forma direta ou indireta, às suas informações e recursos corporativos.

5.2 O ativo “informação”

- Toda informação utilizada pelas empresas Eletrobras é um ativo que possui valor, devendo ser gerenciada adequadamente ao longo de todo seu ciclo de vida (criação, registro, classificação, acesso, manuseio, reprodução, transmissão, guarda e descarte), permitindo que esteja disponível para acesso pelo público adequado, protegida de manipulação indevida, com tratamento adequado de sigilo e acesso e com a possibilidade de se rastrear sua autoria e origem.

5.3 Proprietário da informação

- As empresas Eletrobras são as proprietárias e a detentoras do direito de uso exclusivo das informações geradas, armazenadas, processadas ou transmitidas no ambiente convencional ou de tecnologia.

5.4 Classificação da informação

- As informações utilizadas nas empresas Eletrobras devem ser classificadas a partir de metodologias e critérios definidos em documentos normativos internos específicos, quanto ao seu grau de sigilo ou nível de restrição de acesso, considerando os processos e atividades nas quais estão inseridas, a fim de assegurar que a mesma receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para as empresas Eletrobras.

5.5 Utilização da informação e dos recursos corporativos

- Cabe ao gestor de cada informação determinar a autorização de seu acesso, incluindo os relacionados ao sistema de gestão empresarial, levando em consideração o sigilo adequado e a necessidade de acesso para cada tipo de público, no cumprimento dos objetivos estratégicos das empresas Eletrobras.
- O acesso à informação deve ser autorizado apenas para os colaboradores que necessitem da mesma para o desempenho de suas atividades profissionais.
- Cada colaborador deve acessar apenas as informações ou os sistemas previamente autorizados. Qualquer tentativa não autorizada de acesso consciente a informações ou sistemas deve ser considerada uma falta disciplinar, em acordo com normativo específico de gestão de consequências.
- A credencial (*login* e senha) concedida a um colaborador deve ser de uso individual, intransferível e de conhecimento exclusivo.
- Os recursos corporativos fornecidos pelas empresas Eletrobras, inclusive o correio eletrônico, devem ser utilizados prioritariamente para fins profissionais. Dessa forma, todo e qualquer uso não deve violar leis e normativos competentes, bem como o Código de Ética e de Conduta das Empresas Eletrobras.
- Para garantir o cumprimento desta política, a utilização dos recursos corporativos é registrada e monitorada pelas empresas Eletrobras, não devendo o colaborador ter expectativa de sigilo em sua utilização.

5.6 Proteção da informação

- As empresas Eletrobras orientam, por meio de seu Código de Ética e de Conduta, que os colaboradores devem “preservar a integridade de documentos, registros, cadastros e sistemas de informação das empresas Eletrobras, em todos os meios utilizados pela empresa, tanto físico quanto eletrônico”.
- Os gestores das áreas devem solicitar proteção e controle de acesso físico e lógico aos seus recursos de informação, compatível com o seu nível de criticidade e/ou classificação.
- Todo incidente que afetar a segurança da informação deve ser reportado.
- Os riscos de segurança da informação devem ser identificados, quantificados e priorizados para que se adotem medidas de proteção adequada.

5.7 Sigilo da informação

- As empresas Eletrobras orientam, por meio de seu Código de Ética e de Conduta, que os seus colaboradores não devem “divulgar ou fazer uso de informações privilegiadas estratégicas e confidenciais da empresa em benefício próprio ou de terceiros”, não importando o tipo de mídia ou suporte utilizado.

5.8 Continuidade do uso da informação

- Os recursos utilizados no ambiente convencional ou de tecnologia, onde são realizadas as atividades de gestão, operacionais e de suporte das empresas Eletrobras, devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade definidos.
- Os gestores das áreas devem definir e implantar medidas de prevenção e recuperação para situações de desastre e contingência, contemplando recursos humanos, de tecnologia e de infraestrutura.

5.9 Relacionamentos formais com terceiros

- Todos os relacionamentos formais com terceiros (contratos, convênios, acordos de acionistas, acordos de gestão, formação de consórcios, dentre outros) em que haja o compartilhamento de informações das empresas Eletrobras e/ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos corporativos devem ser precedidos por Termos de Confidencialidade e cláusulas que tratem especificamente da Segurança da Informação.

5.10 Temporalidade da informação

- As empresas Eletrobras devem garantir que qualquer informação com valor comprobatório para fins de auditorias, de conformidade e judiciais seja preservada na forma e pelos prazos demandados, em acordo com normativo específico.

5.11 Capacitação

- As empresas Eletrobras devem incluir a Segurança da Informação em seus programas de capacitação.

5.12 Violações e Penalidades

- As empresas Eletrobras orientam os colaboradores, por meio de seu Código de Ética e de Conduta, que “o descumprimento de algum dos princípios éticos ou compromissos de conduta”, bem como a mera tentativa de burla às diretrizes desta política ou aos controles estabelecidos pela empresa, quando constatada, deve ser tratado como uma violação e 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”.

6 Responsabilidades

- Conselho de Administração da Eletrobras** – aprovar esta política e deliberar sobre as diretrizes estratégicas de segurança da informação norteando todo o processo nas empresas Eletrobras.
- Diretorias Executivas nas empresas Eletrobras** – aprovar os documentos normativos derivados que permitam a implantação desta política.
- Diretoria Executiva da Eletrobras** – aprovar esta política e os documentos normativos derivados que permitam sua implantação.
- Comitê de Segurança da Informação da Eletrobras** – manter as diretrizes desta política, monitorar as ações necessárias para o seu cumprimento, manter os documentos normativos desdobrados desta política e promover a cultura de Segurança da Informação por meio de treinamentos e conscientizações nas empresas Eletrobras.
- Área responsável pela Segurança da Informação na Eletrobras** – coordenar o tratamento de incidentes de Segurança da Informação e, conseqüentemente, acompanhar as investigações e as avaliações dos danos decorrentes da quebra de segurança, apoiar a gestão dos riscos de Segurança da Informação, definindo controles adequados, em conjunto com os gestores das áreas, gerir a matriz corporativa de classificação da informação quanto à restrição de acesso e apoiar a execução das ações estabelecidas pelo Comitê de Segurança da Informação.
- Área responsável pela Segurança da Informação nas empresas Eletrobras** – acompanhar as ações necessárias para o cumprimento desta política, promover a cultura de Segurança da Informação e apoiar a gestão dos riscos de Segurança da Informação, definindo controles adequados, em conjunto com os gestores das áreas.
- Gestores das áreas** – zelar pelas informações produzidas por sua equipe, realizando sua adequada classificação e autorização de acesso e contingência, bem como o mapeamento, implantação e operacionalização de seus controles, fazendo cumprir as diretrizes desta política.
- Colaboradores** – cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, por meio do uso de forma responsável, profissional, ética e legal das informações corporativas, respeitando os direitos e as permissões de uso concedidas pelas empresas Eletrobras.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DAS EMPRESAS ELETROBRAS

- **Áreas de gestão de pessoas** – promover ações de treinamento e desenvolvimento referentes à segurança da informação, incluindo aspectos técnicos, normativos e comportamentais.

7 Disposições Gerais

- O presente documento deve ser lido e considerado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes adotados pelas empresas Eletrobras, incluindo seus anexos. Além disso, esta política deve ser desdobrada em outros documentos normativos específicos, sempre alinhados às diretrizes e princípios aqui estabelecidos.
- As diretrizes aqui estabelecidas devem nortear a atuação, destacadamente, das áreas responsáveis pela tecnologia da informação, tecnologia da automação e segurança da informação das empresas Eletrobras, contribuindo para uma visão única e integrada.
- Deve ser assegurado pelas empresas Eletrobras que esta política e seus documentos normativos complementares sejam amplamente divulgadas aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com a organização e que, direta ou indiretamente, são impactados.
- As empresas Eletrobras devem manter um programa de atualização, de no máximo a cada três anos, dessa política e dos demais instrumentos regulamentares subordinados a ela, visando garantir 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 sua política de negócios.
- Esta política foi aprovada pela Diretoria Executiva da Eletrobras, por meio da Resolução RES-677/2018, de 25/09/2018 e pelo Conselho de Administração, por meio da Deliberação DEL-200/2018, em 28/09/2018.

8 Anexo

- Diretrizes específicas de Controle de Acesso ao SAP das empresas Eletrobras.