Eletrobras

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DAS EMPRESAS ELETROBRAS

Edição 5.0
01/12/2022

Política de Segurança da Informação das Empresas Eletrobras

Área responsável pela emissão

Diretoria de Governança, Riscos e Conformidade / Superintendência de Gestão de Riscos, Controles Internos e Segurança da Informação.

Público-alvo

Colaboradores das empresas Eletrobras que venham a ter acesso, de forma direta ou indireta, a informações e recursos de tecnologia corporativos e operativos.

Aprovação

Resolução RES-501/2022, de 24/10/2022, da Diretoria Executiva da Eletrobras.
Deliberação DEL-168/2022, de 01/12/2022, do Conselho de Administração da Eletrobras.

Repositório

As políticas das empresas Eletrobras podem ser encontradas no *site*:
https://eletrobras.com/pt/Paginas/Estatuto-Politicas-e-Manuais.aspx

Prazo máximo de revisão: 3 anos.

Histórico de edições:

Edição	Aprovação	Principais alterações
1.0	RES-833/2017, de 26/12/2017 e DEL-008/2018, de 29/01/2018.	Não se aplica.
2.0	RES-677/2018, de 25/09/2018 e DEL-200/2018, de 28/09/2018.	Inclusão das diretrizes da Política de Controle de Acesso ao SAP das Empresas Eletrobras, por solicitação do Comitê de Auditoria e Riscos Estatutário (CAE).
3.0	RES-251/2021, de 19/04/2021 e DEL-079/2021, de 29/04/2021.	Ampliação de referências, conceitos e princípios presentes na Lei Geral de Proteção de Dados (LGPD) e no Decreto sobre a Estratégia Nacional de Segurança Cibernética. Retirada do Apêndice para transformação em regulamento.
4.0	RES-076/2022, de 07/03/2022 e DEL-037/2022, de 24/03/2022.	Revisão geral do documento, resultando em correções e adequações de conteúdo para atender demanda do Comitê de Tecnologia Operacional das Empresas Eletrobras (CTOEE), com objetivo de contemplar especificações de segurança da informação para Tecnologia Operacional (TO).
5.0	RES-501/2022, de 24/10/2022 e DEL-168/2022, de 01/12/2022.	Ajustes necessários em razão da alteração da natureza jurídica das empresas Eletrobras, em relação a referências legais e classificação da informação.

Sumário

1 Objetivo

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

2 Referências

2.1 Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD).

2.2 Decreto nº 10.222, de 5 de fevereiro de 2020 – Aprova a Estratégia Nacional de Segurança Cibernética.

2.3 Decreto nº 9.637, de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.

2.4 Decreto nº 3.505/2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

2.5 Portaria GSI/PR Nº 93, de 18 de outubro de 2021 – DOU – Imprensa Nacional (in.gov.br).

2.6 Resolução Normativa Aneel nº 964, de 14 de dezembro de 2021 - Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.

2.7 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.

2.8 Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009 – Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

2.9 ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

2.10 ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação.

2.11 ABNT ISO GUIA 73:2009 – Gestão de riscos.

2.12 Rotina Operacional – Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético (ONS RO-CB.BR.01).

2.13 Código de Conduta Ética e Integridade.

2.14 Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras.

2.15 Política de Gestão de Riscos das Empresas Eletrobras.

2.16 Regulamento de Classificação da Informação das Empresas Eletrobras.

3 Princípios

3.1 Garantia de disponibilidade, para que a informação esteja acessível e utilizável, quando necessário.

3.2 Garantia de integridade da informação, para que não seja modificada ou destruída de maneira não autorizada ou acidental.

3.3 Garantia de confidencialidade da informação, para que esteja disponível ou revelada somente à pessoa física, sistema, órgão ou entidade autorizada e credenciada.

3.4 Garantia de autenticidade de autoria e de origem da informação, para que sejam sempre identificáveis.

4 Diretrizes

4.1 Gestão do ativo "informação"

4.1.1 Toda informação utilizada pelas empresas Eletrobras é um ativo que possui valor e deve ser gerenciada adequadamente ao longo de todo seu ciclo de vida, para que esteja disponível para acesso autorizado, protegida contra manipulação indevida, com tratamento adequado à sua classificação e passível de rastreamento.

4.2 Propriedade e uso da informação

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

4.3 Classificação da informação

4.3.1 As informações utilizadas nas empresas Eletrobras devem ser classificadas a partir de metodologias e critérios definidos no Regulamento de Classificação da Informação das Empresas Eletrobras, considerando os processos e atividades em que estão inseridas, a fim de assegurar que recebam um nível adequado de proteção, conforme valor, requisitos legais e criticidade para as empresas Eletrobras.

4.4 Utilização da informação e dos recursos de tecnologia corporativos e operativos

4.4.1 O gestor da informação deve determinar a autorização de acesso, incluindo os relacionados ao sistema de gestão empresarial, levando em consideração a classificação da informação, no cumprimento dos objetivos estratégicos das empresas Eletrobras.

4.4.2 O acesso à informação deve ser autorizado apenas para os colaboradores e sistemas que dela necessitem para o desempenho de atividades profissionais.

4.4.3 Cada colaborador deve acessar apenas as informações ou os sistemas previamente autorizados. Qualquer tentativa não autorizada de acesso à informação por meio dos recursos de tecnologia corporativos e operativos deve ser investigada e poderá ser considerada uma falta disciplinar.

4.4.4 A credencial (*login* e senha) concedida a um colaborador é de uso individual, intransferível e de conhecimento exclusivo.

4.4.4.1 Nos ativos que não possuam recursos de individualização de acesso, a gestão das credenciais é de responsabilidade do gestor da informação de sua respectiva área, que deve determinar a autorização e a forma de acesso.

4.4.5 Os recursos de tecnologia corporativos e operativos 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 Conduta Ética e Integridade.

4.4.6 Para garantir o cumprimento desta política, a utilização dos recursos de tecnologia corporativos e operativos deve ser registrada e monitorada pelas empresas Eletrobras, não devendo o colaborador ter expectativa de privacidade nessa utilização.

4.5 Proteção da informação

4.5.1 A segurança da informação deve ser obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e recursos de tecnologia.

4.5.2 A Eletrobras orienta, por meio de seu Código de Conduta Ética e Integridade, 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".

4.5.3 O gestor da informação deve providenciar proteção e controle de acesso físico e lógico aos ativos de informação de sua respectiva área, compatíveis com o seu nível de classificação.

4.5.4 Todo incidente que afetar a segurança da informação deve ser registrado conforme orienta o Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras.

4.5.5 Os riscos de segurança da informação devem ser identificados, quantificados e priorizados, para que se adotem medidas de proteção adequada.

4.5.6 As áreas responsáveis pela segurança cibernética devem manter registros atualizados dos indicadores de segurança cibernética, bem como a adequada manutenção do ambiente de tecnologia, dos ativos, das configurações e das soluções de segurança em uso na empresa.

4.5.7 As áreas responsáveis pela segurança cibernética devem fazer acompanhamento das vulnerabilidades dos seus ativos, em atendimento ao Regulamento de Gestão de Vulnerabilidades das Empresas Eletrobras.

4.5.8 As áreas responsáveis pela segurança cibernética devem informar às áreas responsáveis pela segurança da informação, nas empresas Eletrobras, quaisquer dados que se façam necessários para compor relatórios ao mercado ou à administração das empresas Eletrobras.

4.6 Confidencialidade da informação

4.6.1 Os colaboradores das empresas Eletrobras não devem divulgar ou fazer uso de informações de propriedade das empresas Eletrobras, em benefício próprio ou de terceiros, não importando o tipo de mídia ou suporte utilizado. O descumprimento dessa diretrizdeve ser investigado e poderá ser considerado uma falta disciplinar.

4.7 Continuidade do uso da informação

4.7.1 Os recursos de tecnologia corporativos e operativos utilizados nas atividades de gestão, operacionais e de suporte das empresas Eletrobras, que estejam identificados como críticos ao

negócio, devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade definidos.

4.7.2 As empresas Eletrobras devem definir, implementar e testar periodicamente medidas de prevenção e recuperação para situações de desastre e contingência, que devem contemplar os colaboradores e os recursos de tecnologia e de infraestrutura necessários.

4.8 Relacionamentos formais com terceiros

4.8.1 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 ou a concessão de qualquer tipo de acesso aos recursos de tecnologia corporativos e operativos, devem ser precedidos por termos de confidencialidade e conter cláusulas que tratem especificamente de privacidade e segurança da informação.

4.9 Temporalidade da informação

4.9.1 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, pela legislação vigente ou em acordo com normativo específico.

4.10 Capacitação

4.10.1 As empresas Eletrobras devem incluir o tema de segurança da informação em seus programas de capacitação.

4.11 Tratamento de dados pessoais

4.11.1 As empresas Eletrobras devem assegurar o adequado tratamento de dados pessoais, em estrita observância aos termos da Lei Geral de Proteção de Dados (LGPD), nomeando e garantindo o exercício pleno de um encarregado de tratamento de dados pessoais; e estabelecer um canal de atendimento à sociedade civil e de interação com a Autoridade Nacional de Proteção de Dados (ANPD), bem como processos formais de tratamento de incidentes com privacidade dos dados pessoais.

4.12 Violações e penalidades

4.12.1 O descumprimento de qualquer item dessa política de segurança deve ser investigado e poderá ser considerado uma falta disciplinar, conforme Código de Conduta Ética e Integridade.

5 Responsabilidades

5.1 Conselho de Administração da Eletrobras (CA) – aprovar esta política e deliberar sobre as diretrizes estratégicas de segurança da informação para nortear o processo de implementação nas empresas Eletrobras.

5.2 Diretoria Executiva da Eletrobras (DEE) – aprovar esta política e, quando aplicável, os documentos normativos derivados que permitam sua implementação.

5.3 Diretorias Executivas nas empresas Eletrobras – aprovar, quando aplicável, os documentos normativos derivados que permitam a implementação desta política.

5.4 Área responsável pela segurança da informação da Eletrobras *holding* – elaborar políticas e regulamentos que padronizem ações de segurança da informação nas empresas Eletrobras e coordenar o Comitê de Segurança da Informação das Empresas Eletrobras (CESIE).

5.5 Comitê de Segurança da Informação da Eletrobras (CESIE) – manter as diretrizes desta política e monitorar as ações necessárias para o seu cumprimento; manter os documentos normativos desdobrados desta política, definir e monitorar o *framework* de segurança da informação, realizar o planejamento anual de segurança da informação e promover a cultura de segurança da informação por meio de treinamentos e campanhas de conscientização na Eletrobras *holding*.

5.6 Comitê de Tecnologia Operacional das Empresas Eletrobras (CTOEE) – manter as diretrizes desta política no âmbito da TO, monitorar as ações necessárias para o seu cumprimento e manter os documentos normativos desdobrados desta política.

5.7 Comitê de Tecnologia da Informação, Automação e Telecomunicação do Sistema Eletrobras (Cotise) – manter a Política Integrada de Tecnologia da Informação, Automação e Telecomunicação das Empresas Eletrobras, aprovar suas diretrizes específicas, orientar e acompanhar o estabelecimento e a observância de processos, controles, modelos, padrões e ferramentas necessários à sua implementação e analisar as questões específicas apresentadas pelos representantes das empresas para posterior aplicação nas empresas Eletrobras.

5.8 Áreas responsáveis pela segurança da informação nas empresas Eletrobras – gerir, em sua respectiva empresa, os processos e o planejamento de ações de desdobramento desta política; promover treinamentos e campanhas de conscientização em segurança da informação; coordenar o tratamento de incidentes de segurança da informação; apoiar a gestão dos riscos de segurança da informação, definindo controles adequados em conjunto com as áreas proprietárias de risco; coordenar a implementação e a manutenção do plano de continuidade de negócio em relação à disponibilidade de informações; prestar suporte à primeira linha de defesa; gerenciar o processo de gestão da privacidade e proteção de dados pessoais ; e apoiar e participar da execução das ações estabelecidas pelo Comitê de Segurança da Informação das Empresas Eletrobras (CESIE).

5.9 Áreas responsáveis pela segurança cibernética nas empresas Eletrobras – atender as demandas da área responsável pela segurança da informação da respectiva empresa; gerir os indicadores cibernéticos; comunicar, registrar e tratar os incidentes cibernéticos; alinhar o planejamento de projetos e iniciativas cibernéticas com a área responsável pela segurança da informação e atender às solicitações do coordenador do Grupo de Resposta e Tratamento a Incidentes de Segurança da Informação (GRSI); planejar a segurança cibernética do ambiente em que atuam, definindo as configurações tecnológicas necessárias para o alcance da segurança da informação.

5.10 Gestores das áreas – zelar pelas informações produzidas por sua equipe, realizando sua adequada classificação e autorização de acesso e contingência, bem como o mapeamento, a implantação e a operacionalização de seus controles, fazendo cumprir as diretrizes desta política.

5.11 Áreas responsáveis pela segurança física das empresas Eletrobras – prevenir e proteger instalações e ativos de informação contra acessos físicos não autorizados, danos ou comprometimento de informações; avaliar, regularmente, o ambiente; e encaminhar à área responsável pela segurança da informação da empresa relatório das vulnerabilidades encontradas nas medidas de segurança física.

5.12 Colaboradores – cumprir esta política e os demais instrumentos regulamentares relacionados, por meio do uso das informações corporativas e operativas de forma responsável, profissional, ética e legal, respeitando os direitos e as permissões de uso concedidas pelas empresas Eletrobras.

6 Conceitos

6.1 Ambiente convencional – composto por ativos de informação (como fotos, microfilmes,

documentos impressos, projetos físicos, registros não digitais em geral) que não façam parte do ambiente de tecnologia.

6.2 Ambiente de tecnologia – composto por meios de armazenamento, transmissão e processamento de informações, assim como pelos equipamentos e sistemas utilizados para tal, que empreguem tecnologias eletrônicas ou digitais.

6.3 Área – unidade organizacional formal, que possui determinadas atribuições e responsabilidades (diretoria, assessoria, superintendência, departamento, divisão).

6.3.1 Área responsável pela segurança cibernética – uma ou mais áreas formalmente responsáveis pela segurança cibernética em TI, TO ou TE.

6.3.2 Área responsável pela segurança da informação – área formalmente responsável pela segurança da informação.

6.4 Área proprietária de risco (*risk owner*) – unidade organizacional que possui autoridade e responsabilidade sobre o gerenciamento do risco.

6.5 Ativo – qualquer recurso que tenha valor para as empresas Eletrobras.

6.5.1 Ativo de informação – dados, informações e seus meios de armazenamento, transmissão e processamento de informações, os equipamentos e sistemas utilizados para tal, os locais onde se encontram esses meios, assim como os recursos humanos que a eles têm acesso.

6.6 Autenticidade – propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

6.7 Ciclo de vida da informação – compreende a utilização da informação, desde o momento em que ela é gerada, rotulada, manipulada, armazenada, classificada e transmitida, até a sua destruição.

6.8 Classificação da informação – processo de identificar e definir níveis e critérios adequados de proteção das informações, com objetivo de garantir sua confidencialidade, integridade e disponibilidade.

6.9 Colaborador – diretores, conselheiros, empregados, membros de comitês estatutários, prestadores de serviço, estagiários e prestadores de serviço não eventualque atuem nas empresas Eletrobras.

6.10 Confidencialidade – propriedade que garante que a informação seja acessada somente por ativos de informação autorizados pelo gestor da informação.

6.11 Criticidade – categorização do ativo quanto ao nível de impacto dos riscos associados ao negócio.

6.12 Disponibilidade – propriedade que garante o acesso às informações e aos recursos associados, e aos ativos de informação autorizados, quando necessário.

6.13 Gestor da área – responsável formal titular da unidade organizacional.

6.14 Gestor da informação – titulares das áreas que desempenham atividades gerenciais e titulares dos órgãos executivos de direção superior, conforme norma específica.

6.15 Grupo de Resposta e Tratamento a Incidentes de Segurança da Informação (GRSI) – grupo definido no Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras.

6.16 Incidente de segurança da informação – qualquer evento adverso, confirmado ou sob suspeita, que afete a proteção dos sistemas de informação e que comprometa ou tenha potencial para comprometer a disponibilidade, a integridade, a confidencialidade, a autenticidade, a legalidade e/ou a privacidade da informação.

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

6.18 Linha de defesa – conceito que auxilia na estruturação e definição clara dos papéis e responsabilidades, de forma que a atuação passe a ser integrada. Dividido em três linhas de defesa:

1ª linha: responsável por implementar e operacionalizar os controles para mitigar os riscos de segurança da informação (área responsável pela segurança cibernética);

2ª linha: responsável por definir as diretrizes e monitorar o cumprimento pela primeira linha (área responsável pela segurança da informação);

3ª linha: realiza avaliações independentes que permeiam o ciclo completo de gestão de riscos (auditoria interna).

6.19 Privacidade – propriedade da informação privada que só possa ser acessada por terceiros com conhecimento e autorização prévios das pessoas de que ela trata.

6.20 Recurso de tecnologia corporativo – qualquer ativo de informação, exceto recursos humanos, no ambiente convencional ou de tecnologia das empresas Eletrobras, pertencente a Tecnologia da Informação, Automação e Telecomunicação (TIC).

6.21 Recurso de tecnologia operativo – toda a infraestrutura computacional e de telecomunicações de tempo real e histórico, que atende à sala de controle e outras áreas interessadas e que está protegida pelos firewalls operativos. (REG-TO)

6.22 Restrição de acesso – restrição da interação entre ativos de informação, impedindo o acesso físico, o acesso lógico ou o fluxo de informações entre os ativos de informação (como, por exemplo, restrição de acesso entre pessoas e arquivos, entre serviços, entre pessoas).

6.23 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.

6.24 Risco de segurança da informação – potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças.

6.25 Segurança cibernética – ações sobre pessoas, tecnologias e processos, com objetivo de viabilizar que os ativos de informação dos ambientes de tecnologia sejam capazes de resistir a incidentes que possam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

6.26 Segurança da informação – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, dos ambientes convencional e de tecnologia, por meio de métodos que visam integrar aos processos institucionais estratégicos, operacionais e táticos 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 e segurança organizacional.

6.27 Segurança física – medidas físicas destinadas a impedir, detectar e responder ao acesso

não autorizado a pessoas, bens, valores, equipamentos, e instalações relacionadas aos ativos.

6.28 Tecnologia Operacional (TO) – conjunto de sistemas de automação e de redes de comunicação operacionais necessários à gestão dos ativos, monitoração, e controle de operações industriais, aplicados nos centros de operação, subestações e usinas, e seus processos e dispositivos; estão incluídos neste rol os equipamentos "*stand-alone*" de monitoração e controle.

6.29 Unidade organizacional – componente da estrutura organizacional da empresa que se encontra subordinado, direta ou indiretamente, a um órgão executivo de direção superior ou a órgão de direção colegiada.

7 Disposições Gerais

7.1 As diretrizes aqui estabelecidas devem nortear a atuação, destacadamente, das áreas responsáveis pela tecnologia da informação, pela tecnologia operacional e pela segurança da informação das empresas Eletrobras, contribuindo para uma visão única e integrada.

7.2 As empresas Eletrobras devem adequar seus documentos normativos e os controles que se fizerem necessários em consonância com o estabelecido nesta política. O prazo máximo para adequação é de 90 dias a partir da aprovação pelo Conselho de Administração da Eletrobras (CA).

7.3 Esta política pode ser desdobrada em regulamentos unificados e válidos para todas as empresas Eletrobras e ainda em documentos normativos internos específicos em cada empresa Eletrobras, sempre alinhados aos princípios e diretrizes aqui estabelecidos.

7.3.1 O presente documento deve ser lido, considerado e aplicado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes adotados pelas empresas Eletrobras, incluindo seus anexos.

7.4 Deve ser assegurado pelas empresas Eletrobras que esta política e seus documentos normativos complementares sejam amplamente divulgados aos seus colaboradores, visando a sua aplicação por todos que se relacionam com a organização e que, direta ou indiretamente, são impactados.

7.5 Esta política e demais instrumentos regulamentares subordinados a ela, excepcionando-se às regras internas que regem as revisões de documentos normativos das empresas Eletrobras, devem ser atualizados no prazo máximo de 3 anos ou sempre que houver necessidade, visando garantir que os requisitos técnicos e legais de segurança implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente e alinhados às diretrizes que conduzem o desenvolvimento dos nossos negócios, presentes no nosso planejamento estratégico.