Eletrobras

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DAS EMPRESAS ELETROBRAS

Edição 3.0
29/04/2021

Política de Segurança da Informação das Empresas Eletrobras

Área responsável pela emissão

Superintendência de Gestão de Riscos, Controles Internos e Segurança da Informação / Departamento de Gestão e Segurança da Informação.

Público-alvo

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

Aprovação

Resolução RES-251/2021, de 19/04/2021, da Diretoria Executiva da Eletrobras.
Deliberação DEL-079/2021, de 29/04/2021, 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

Direitos de autor e confidencialidade

Prazo máximo de revisão: 3 anos

Histórico de edições

Edição	Aprovação	Principais alterações
1.0	RES-833/2017, de 26/12/2017.	Não se aplica.
1.0	DEL-008/2018, de 29/01/2018.	Não se aplica.
2.0	RES-677/2018, de 25/09/2018.	Comportar as diretrizes da Política de Controle de Acesso ao SAP das empresas Eletrobras, por solicitação do Comitê de Auditoria e Riscos Estatutário – CAE.
2.0	DEL-200/2018, de 28/09/2018.	Idem acima.
3.0	RES-251/2021, de 19/04/2021 e DEL-079/2021, de 29/04/2021.	Ampliação das referências, conceitos e princípios presentes na LGPD e no Decreto sobre a Estratégia Nacional de Segurança Cibernética. Retirada do Apêndice para transformação em regulamento.

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, a 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 nº 93, de 26 de setembro de 2019, Glossário de Segurança da Informação.

2.6 Portaria nº 09 GSI, de 9 de março de 2018, NC 14 IN01 Computação em Nuvem.

2.7 Instrução Normativa GSI Nº 3, de 6 de março de 2013 – Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

2.8 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.

2.9 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.

2.10 ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

2.11 ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

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

2.13 Código de Conduta Ética e Integridade das Empresas Eletrobras.

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

2.15 Política de Gestão de Riscos das Empresas Eletrobras.

3 Princípios

3.1 Garantia de disponibilidade, para que a informação esteja acessível e utilizável sob demanda a toda empresa.

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 não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

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

4 Diretrizes

4.1 O 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 pelo público adequado, protegida contra manipulação indevida, com tratamento adequado ao seu grau de sigilo ou restrição de acesso e passível de rastreamento.

4.2 Proprietário 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 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 essas informações recebam um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para as empresas Eletrobras.

4.4 Utilização da informação e dos recursos corporativos

4.4.1 O gestor de cada informação deve determinar a autorização de 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 da Eletrobras.

4.4.2 O acesso à informação deve ser autorizado apenas para os colaboradores que dela necessitem para o desempenho de suas 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 ou sistema deve 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.

4.4.5 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 Conduta Ética e Integridade das Empresas Eletrobras.

4.4.6 Para garantir o cumprimento desta política, a utilização dos recursos corporativos deve ser registrada e monitorada pelas empresas Eletrobras, não devendo o colaborador ter expectativa de sigilo em sua 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 sistemas.

4.5.2 A Eletrobras orienta, por meio de seu Código de Conduta Ética e Integridade das Empresas Eletrobras, 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 Os gestores das áreas devem providenciar proteção e controle de acesso físico e lógico aos seus recursos de informação, compatível com o seu nível de criticidade e/ou classificação.

4.5.4 Todo incidente que afetar a segurança da informação deve ser reportado à área responsável por segurança da informação.

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 de segurança cibernética devem manter registros atualizados dos indicadores de segurança da informação, bem como a adequada manutenção da arquitetura cibernética, dos ativos tecnológicos, das configurações e das soluções de segurança em uso na empresa.

4.5.7 As áreas de segurança cibernética devem informar às áreas de segurança da informação quaisquer dados que se façam necessários para compor relatórios à administração das empresas Eletrobras.

4.6 Sigilo da informação

4.6.1 Os colaboradores das empresas não devem divulgar ou fazer uso de informações corporativas da empresa em benefício próprio ou de terceiros, não importando o tipo de mídia ou suporte utilizado.

4.7 Continuidade do uso da informação

4.7.1 Os recursos de ambiente convencional ou de tecnologia utilizados nas atividades de gestão, operacionais e de suporte das empresas Eletrobras, devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade definidos.

4.7.2 Os gestores das áreas devem definir e implementar 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 e/ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos corporativos 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, em acordo com normativo específico.

4.10 Capacitação

4.10.1 A Eletrobras deve incluir a 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 nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), nomeando e garantindo o exercício pleno de um encarregado de tratamento de dados pessoais, estabelecer um canal de atendimento à sociedade civil e de interação com a Autoridade Nacional de Proteção de Dados (ANPD) e processos formais de tratamento de incidentes com privacidade dos dados pessoais.

4.12 Violações e penalidades

4.12.1 A Eletrobras orienta os colaboradores, por meio de seu Código de Conduta Ética e Integridade das Empresas Eletrobras, 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".

5 Responsabilidades

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

5.2 Diretorias Executivas nas empresas Eletrobras – aprovar os documentos normativos derivados que permitam a implementação desta política.

5.3 Diretoria Executiva da Eletrobras – aprovar esta política e os documentos normativos derivados que permitam sua implementação.

5.4 **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 na Eletrobras *holding*.

5.5 **Área responsável pela segurança da informação na 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).

5.6 **Área responsável pela segurança da informação nas empresas Eletrobras** – no âmbito de sua empresa, gerir os processos e planejamento de ações de desdobramento desta política, promover treinamentos e campanhas de conscientização em SI, coordenar o tratamento de incidentes de SI, apoiar a gestão dos riscos de SI definindo controles adequados em conjunto com os *risk owners*, gerir a matriz de classificação da informação, coordenar a implementação e manutenção do Plano de Continuidade de Negócio em relação à disponibilidade de informações, prestar suporte a 1ª linha de defesa, atuar como encarregado pelo tratamento de dados pessoais; e, apoiar e participar da execução das ações estabelecidas pelo Comitê de Segurança da Informação.

5.7 **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.

5.8 **Responsável pela segurança cibernética** – atender as demandas da área responsável pela segurança da informação, gerir os indicadores cibernéticos, comunicar os incidentes, alinhar o planejamento de projetos e iniciativas cibernéticas com área responsável pela segurança da informação e atender às solicitações do coordenador do GRSI – Grupo de Resposta e Tratamento a Incidentes de Segurança da Informação, planejar a segurança cibernética do ambiente em que atuam, definindo as configurações tecnológicas necessárias para o alcance da segurança da informação.

5.9 **Responsável pela segurança física** – prevenir e proteger instalações e ativos de informação contra acessos não autorizados, danos ou comprometimento de informações. Compete ainda avaliar regularmente o ambiente e encaminhar relatório das vulnerabilidades encontradas nas medidas de segurança física ao responsável pela segurança da informação.

5.10 **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.

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

6 Conceitos

6.1 Artefato malicioso

Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes de computadores.

6.2 Ataque

Tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível.

6.3 Ativo

Qualquer recurso que tenha valor para as empresas Eletrobras.

6.4 Ativo de informação

Dados, informações e seus meios de armazenamento, transmissão e processamento, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

6.5 Colaborador

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

6.6 Espaço cibernético

Espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente.

6.7 Gestor de informação

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

6.8 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.

6.9 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 segurança da informação.

6.10 Informação

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

6.11 Privacidade

Propriedade que exige o direito à reserva de informações pessoais, além da prerrogativa de controlar a exposição e disponibilidade de informações acerca de si mesmo (regulação dos limites).

6.12 Proprietário da informação

Gestor de unidade organizacional responsável pela produção ou tratamento das informações em seus processos de negócio.

6.13 Proprietário do risco (ou *risk owner*)

Colaborador que possui autoridade e responsabilidade pelo gerenciamento de um ou mais Riscos de Segurança da Informação.

6.14 Risco de segurança da informação

Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças.

6.15 Segurança cibernética

Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de 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.

6.16 Segurança da informação

Ações que objetivam viabilizar e assegurar a disponibilidade, integridade e confidencialidade da informação.

6.17 Segurança física

Medidas físicas destinadas a impedir, detectar e responder ao acesso não autorizado a pessoas, bens, valores, equipamento, instalações relacionadas aos ativos de informação.

6.18 Titular

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

6.19 Usuário

Pessoa física, ou responsável por conta de serviço, habilitada para acessar os ativos de informação de uma ou mais das empresas Eletrobras.

6.20 Violação

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

7 Disposições Gerais

7.1 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. Além disso, esta política deve ser desdobrada em outros documentos normativos específicos, sempre alinhados às diretrizes e princípios aqui estabelecidos.

7.2 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.

7.3 As empresas Eletrobras devem adequar seus documentos normativos e os controles que se fizerem necessários em consonância com o estabelecido nesta política no prazo máximo de 180 dias a partir da aprovação pelo Conselho de Administração da Eletrobras.

7.4 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.

7.5 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.

7.6 Esta política, e demais instrumentos regulamentares subordinados a ela, devem ser atualizados dentro do 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.