PLANO DE **SEGURANÇA DA INFORMAÇÃO** DA EMBRAPA

Embrapa

Empresa Brasileira de Pesquisa Agropecuária
Ministério da Agricultura e Pecuária

PLANO DE **SEGURANÇA DA INFORMAÇÃO** DA EMBRAPA

Embrapa
Brasília, DF
2025

O Plano de Segurança da Informação é uma publicação institucional
da Empresa Brasileira de Pesquisa Agropecuária (Embrapa).

Embrapa
Gerência-Geral de Governança Corporativa e Informação

Parque Estação Biológica
Av. W3 Norte (final)
70770-901 Brasília, DF
www.embrapa.br
www.embrapa.br/fale-conosco/sac

Elaboração de texto

Ana Luiza Dias
Andrea Fonseca Rosa Naves
Beatriz de Campos Lorentz
Carlos Fernando Assis Paniago
Emerson de Stefani
Francisco de Assis Monteiro Freire
Frederico dos Santos Silva
Lânia Márcia de Almeida
Marina Mendes Gomes Pereira
Paulo Sérgio Silva Santos

Responsável pela editoração

Coordenação editorial
Cristina Pucci Hercos
Alessandra Rodrigues da Silva
Juliana Meireles Fortaleza

Edição executiva
Cristiane Pereira de Assis

Revisão de texto
Everaldo Correia da Silva Filho
Maria Cristina Ramos Jubé

Normalização bibliográfica
Márcia Maria Pereira de Souza (CRB 1/1441)
Rejane Maria de Oliveira Cechinel Darós

Projeto gráfico, diagramação e capa
Carlos Eduardo Felice Barbeiro

Publicação digital (2025): PDF

Dados Internacionais de Catalogação na Publicação (CIP)
Embrapa, Gerência-Geral de Governança Corporativa e Informação

Embrapa.
Plano de segurança da informação da Embrapa / Embrapa. – Brasília, DF : Embrapa, 2025.
PDF (51 p.)

1. Proteção de dados. 2. Pessoas. 3. Infraestrutura de tecnologia da informação. 4. Infraestrutura física. 5. Processos. I. Título. II. Gerência-Geral de Governança Corporativa e Informação.

CDD (21. ed.) 658.472

Rejane Maria de Oliveira Cechinel Darós (CRB-1/2913)

APRESENTAÇÃO

A segurança da informação (SI) não se refere apenas aos sistemas computacionais, documentos eletrônicos, redes de computadores e infraestruturas de tecnologia da informação e comunicação (TIC). Ela também está relacionada à infraestrutura física, à proteção de dados e a todo tipo de informação que gera valor para a organização, independentemente do meio, suporte ou formato. Dessa forma, por definição, a SI está apoiada em quatro pilares: pessoas, infraestrutura de tecnologia da informação (TI), infraestrutura física e processos.

As normas e boas práticas referentes à SI recomendam a adoção de medidas para proteger as informações e conhecimentos estratégicos das organizações, os quais irão resultar em tecnologias, produtos e serviços, objetos de seus negócios e sua missão.

Nesse contexto, informação é o resultado do processamento, manipulação e organização de dados capazes de gerar conhecimentos, valores e inovações a serem apropriados por países, instituições e pessoas que deles necessitam.

As medidas e controles requerem que todos na organização — gestores, empregados e colaboradores — estejam atentos e sensibilizados para adotarem comportamentos e atitudes favoráveis à segurança e à proteção das informações e conhecimentos com os quais lidam diariamente.

O Plano de Segurança da Informação (PSI) aqui proposto contém cinco principais temas: pessoas, dados, documentos, infraestrutura de TIC e infraestrutura física. Este PSI é um documento operacional com o objetivo de apresentar procedimentos e ações necessárias para prevenir e responder aos incidentes de SI, garantindo a proteção, confidencialidade, integridade e disponibilidade dos ativos de informação da Embrapa.

Silvia Maria Fonseca Silveira Massruhá
Presidente da Embrapa

SUMÁRIO

PESSOAS

A grande maioria dos incidentes de segurança de informação (SI) ocorre por ação ou inação das pessoas, de forma que se torna imprescindível a adoção de medidas seguras quanto à seleção, à movimentação e ao desligamento ou transferência de pessoas, além de fomentar padrões de comportamento profissional e ético adequados à salvaguarda das informações sensíveis da Empresa, bem como oferecer treinamento contínuo dos empregados e colaboradores da Embrapa sobre SI.

Matriz de riscos

Esta seção apresenta a matriz de riscos resultante do processo de análise de riscos realizado para identificar, avaliar e priorizar potenciais ameaças relacionadas ao tema pessoas (Tabela 1). A matriz foi elaborada com base na Metodologia de Gestão de Riscos Corporativos da Embrapa (Embrapa, 2025).

Tabela 1. Matriz de riscos relacionada ao tema pessoas.

Processo	Gestão de Pessoas
Objetivo	Propor as diretrizes táticas de recrutamento, seleção, treinamento e desempenho de pessoas em alinhamento com as diretrizes da governança corporativa.
Ativo	Pessoas

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Perda de dados	Não observância da Norma de Acesso e Tratamento da Informação e/ou do Processo de Gestão de Dados de Pesquisa e/ou Política de Governança de Dados, Informação e Conhecimento da Embrapa; ausência de controle de acesso aos sistemas e aos repositórios de dados; falta de treinamento e conscientização sobre segurança da informação; conduta antiética ou delituosa.	Impossibilidade de recuperação dos dados, reúso e compartilhamento; prejuízo à imagem da Empresa; prejuízo financeiro e científico.	Norma de Acesso e Tratamento da Informação; Processo de Gestão de Dados de Pesquisa; Norma de Uso de Dados para Negócios da Embrapa; Política de Governança de Dados, Informação e Conhecimento da Embrapa; melhores práticas de procedimentos de backup.	Média	Alto	Alto	Tratar
R02	Vazamento ou roubo de dados ou informações de caráter estratégico para soberania nacional	Não observância da Norma de Acesso e Tratamento da Informação e/ou do Processo de Gestão de Dados de Pesquisa e/ou Política de Governança de Dados, Informação e Conhecimento da Embrapa; ausência de controle de acesso aos sistemas e aos repositórios de dados; falta de treinamento e conscientização sobre segurança da informação, atitude antiética ou delituosa.	Prejuízo à imagem da Empresa; prejuízo financeiro e científico.	Norma de Acesso e Tratamento da Informação; Processo de Gestão de Dados de Pesquisa; Código de Conduta, Ética e Integridade da Embrapa; Norma de Uso de Dados para Negócios da Embrapa; Política de Governança de Dados, Informação e Conhecimento da Embrapa; contrato individual de trabalho.	Média	Alto	Alto	Tratar
R03	Adulteração de dados e/ou documentos	Não observância da Norma de Acesso e Tratamento da Informação e/ou do Processo de Gestão de Dados de Pesquisa e/ou Política de Governança de Dados, Informação e Conhecimento da Embrapa; ausência de controle de acesso aos sistemas e aos repositórios de dados; falta de treinamento e conscientização sobre segurança da informação, atitude antiética ou delituosa.	Impossibilidade de recuperação dos dados, reúso e compartilhamento; prejuízo à imagem da Empresa; prejuízo financeiro e científico.	Norma de Acesso e Tratamento da Informação; Processo de Gestão de Dados de Pesquisa; Código de Conduta, Ética e Integridade da Embrapa; Norma de Uso de Dados para Negócios da Embrapa; Política de Governança de Dados, Informação e Conhecimento da Embrapa; contrato individual de trabalho.	Média	Alto	Alto	Tratar

Prevenção

Durante o processo de admissão do empregado ou colaborador, a área de gestão de pessoas deve:

- Comparar as informações do currículo do candidato com os documentos apresentados.
- Em caso de dúvida, consultar sites, como o Google e Plataforma Lattes.
- Solicitar ajustes, caso sejam identificadas discrepâncias nas informações apresentadas.
- Conferir a autenticidade das cópias dos documentos que comprovam as qualificações acadêmica e profissional do candidato e confirmar a sua veracidade.
- Em caso de dúvida, certificar-se da veracidade, com o Ministério da Educação (MEC) e as instituições de ensino, dos documentos referentes à comprovação de escolaridade e formação acadêmica.

O processo de admissão de empregados, bem como o de contratação de colaboradores, deve assegurar que tanto empregados como colaboradores entendam suas responsabilidades e estejam de acordo com os papéis para os quais foram selecionados.

A área de gestão de pessoas, quando da contratação, deve alertar ao candidato sobre suas responsabilidades e respectivas sanções constantes no contrato de trabalho, bem como no Código de Conduta Ética e nos documentos que tratam da SI.

As áreas de SI e de gestão de pessoas da Embrapa devem disponibilizar, para todos os empregados, treinamentos regulares sobre boas práticas de SI, como o uso adequado dos sistemas, a importância das senhas fortes e o reconhecimento de possíveis ameaças. Adicionalmente, devem incentivar uma cultura organizacional que valorize a SI e encoraje os empregados a relatar qualquer incidente ou comportamento suspeito.

A área de gestão de pessoas, em conjunto com a área responsável pela SI, deve estabelecer controles de acesso aos sistemas e aos repositórios de dados, de acordo com o perfil do empregado ou colaborador e suas funções na Empresa.

Durante o período de afastamento do empregado ou colaborador por férias ou outro motivo, a área de gestão de pessoas, em conjunto com a área responsável pela SI, deve adequar os controles de acesso aos sistemas e aos repositórios de dados, de acordo com a situação de afastamento.

As credenciais de segurança e o acesso a sistemas e aos repositórios de dados, bem como aos locais restritos, só serão permitidos a empregados e colaboradores que estejam em efetivo exercício de suas funções.

Todo empregado ou colaborador que for desligado definitivamente deve ter suas credenciais de segurança e acesso aos sistemas e aos repositórios de dados revogados, devolvendo ao responsável pela continuidade de suas ações ou ao seu superior imediato todo e qualquer ativo que esteja sob a posse do empregado ou colaborador desligado, além de documentos institucionais e/ou processos de trabalho de condução individual.

Os empregados que forem movimentados, transferidos ou cedidos devem ter suas credenciais de segurança e acesso aos sistemas e aos repositórios de dados readequados a sua atual lotação.

Detecção

A comunicação inicial de um incidente de SI deve ser feita por qualquer fonte ou pessoa interna ou externa à Embrapa. A comunicação realizada por via diferente daquela diretamente ligada ao responsável pelo processo ou sistema afetado, em hipótese alguma, poderá ser utilizada como motivo para alegar desconhecimento do incidente.

Os empregados e colaboradores são responsáveis por garantir a segurança das informações da Embrapa a que tenham acesso e por reportar à área responsável pela SI os incidentes de que tenham conhecimento, informando suas consequências e circunstâncias.

Cabe aos responsáveis formais pelas áreas de negócio, entre outras, as seguintes responsabilidades:

- Gerenciar o cumprimento da política de segurança da organização por parte de seus subordinados e colaboradores.
- Identificar os desvios praticados e adotar as medidas corretivas apropriadas.
- Proteger, em âmbito físico e lógico, os ativos de informação e de processamento da organização relacionados à atuação de seu setor.
- Comunicar formalmente à área responsável pela SI quais os empregados e colaboradores, sob sua supervisão, que podem acessar as informações sigilosas da organização, seguindo as normas de classificação de informações e os perfis de cada cargo.
- Comunicar imediatamente à área responsável pela SI o descumprimento por parte de seus subordinados das normas e da política de SI.

Tratamento

Uma vez detectado um incidente de perda, vazamento, roubo ou adulteração de dados ou informação, esse incidente deve ser tratado e analisado para que sejam, na medida do possível, preservadas todas as suas evidências, possibilitando posteriormente o rastreamento e identificação de suas causas.

O tratamento e a análise do incidente devem ser realizados observando-se a definição dos seguintes atributos:

- Unidade e setor onde ocorreu o incidente.
- E-mail, telefone ou outro contato disponível do informante do incidente.
- Data e horário que incidente foi identificado.
- Descrição e consequência do incidente.
- Ativo afetado pelo incidente.
- Responsável pelo ativo afetado.
- Criticidade do incidente.

Resposta

A partir da confirmação de um incidente de SI, cuja causa tenha sido gerada por um empregado ou colaborador, deve ser feita uma rápida avaliação do risco de propagação da ameaça que o causou, bem como agir para que a ameaça não se propague e executar as seguintes ações:

- Restabelecer os serviços afetados no menor tempo possível.
- Atualizar sistemas operacionais, softwares antivírus e todos os outros ativos de TIC, quando o incidente for de natureza cibernética.
- Recuperar os dados a partir das cópias backups dos sistemas e repositórios de dados de PD&I ou de publicações que contenham os dados perdidos; ou, ainda, de mídias alternativas que eventualmente tenham sido utilizadas para a guarda dos dados.
- Apurar as responsabilidades de acordo com as leis, normas vigentes e os termos de compromisso e confidencialidade firmados pelo agente causador do incidente.

- Buscar a proibição da utilização por terceiros dos dados vazados ou roubados, utilizando-se as leis pertinentes e os fundamentos dos direitos de propriedade intelectual e autoral.

Pós-incidente

Após a resposta ao incidente, deve ser agendada uma reunião de lições aprendidas entre os envolvidos nos processos afetados pelo incidente, a área responsável pela SI na Embrapa e a área responsável pela gestão de pessoas, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos, inclusive deste Plano de Segurança da Informação (PSI).

DADOS DE PESQUISA, DESENVOLVIMENTO E INOVAÇÃO

A Embrapa é uma empresa de ciência e tecnologia que, como tal, tem nos dados decorrentes de suas atividades de pesquisa, desenvolvimento e inovação (PD&I) seu principal ativo. Por isso, proteger os dados de PD&I de incidentes de SI torna-se imperioso, para garantir que a Empresa atinja o objetivo de gerar valor e soluções para a ciência agropecuária brasileira e mundial.

Matriz de riscos

Esta seção apresenta a matriz de riscos resultante do processo de análise de riscos realizado para identificar, avaliar e priorizar potenciais ameaças relacionadas ao tema de dados de pesquisa, desenvolvimento e inovação (Tabela 2). A matriz foi elaborada com base na Metodologia de Gestão de Riscos Corporativos da Embrapa (Embrapa, 2025).

Tabela 2. Matriz de riscos para dados de pesquisa, desenvolvimento e inovação.

Processo	Gestão de Dados
Objetivo	Possibilitar à Embrapa governar seus dados, garantindo guarda, proteção, segurança, qualidade, integridade e geração de valor para a Empresa e para a ciência.
Ativo	Dados de PD&I

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Perda de dados	Não observância da Norma de Acesso e Tratamento da Informação e/ou do Processo de Gestão de Dados de Pesquisa e/ou Política de Governança de Dados, Informação e Conhecimento da Embrapa; falta de preparo da equipe em relação à segurança de dados; falta de backup e desastres naturais.	Impossibilidade de recuperação dos dados, reúso e compartilhamento; prejuízo à imagem da Empresa; prejuízo financeiro e científico.	Norma de Acesso e Tratamento da Informação; Processo de Gestão de Dados de Pesquisa; Norma de Uso de Dados para Negócios da Embrapa; Política de Governança de Dados, Informação e Conhecimento da Embrapa; melhores práticas de procedimentos de backup.	Média	Alto	Alto	Tratar
R02	Vazamento ou roubo de dados	Não observância da Norma de Acesso e Tratamento da Informação e/ou do Processo de Gestão de Dados de Pesquisa e/ou Política de Governança de Dados, Informação e Conhecimento da Embrapa; falta de preparo da equipe em relação à segurança de dados.	Perda de oportunidades científicas, patentes, direito autoral e soberania nacional; desgaste e descredibilidade da imagem e marca da Empresa; divulgação indevida de dados por terceiros.	Norma de Acesso e Tratamento da Informação; Processo de Gestão de Dados de Pesquisa; Código de Conduta, Ética e Integridade da Embrapa; Norma de Uso de Dados para Negócios da Embrapa; Política de Governança de Dados, Informação e Conhecimento da Embrapa; contrato individual de trabalho; política/cartilha sobre segurança da informação vigente.	Média	Alto	Alto	Tratar
R03	Indisponi-bilidade de dados	Não observância da Norma de Acesso e Tratamento da Informação e/ou do Processo de Gestão de Dados de Pesquisa e/ou Política de Governança de Dados, Informação e Conhecimento da Embrapa; despreparo da equipe em relação à segurança de dados; indisponibilidade de redes e inoperacionalidade de sistemas.	Impossibilidade de acesso, reúso e compartilhamento de dados; dificuldade no atendimento de demandas externas e internas; impedimento da continuidade de processos e pesquisas.	Norma de Acesso e Tratamento da Informação; Processo de Gestão de Dados de Pesquisa; Norma de Uso de Dados para Negócios da Embrapa; Política de Governança de Dados, Informação e Conhecimento da Embrapa.	Média	Alto	Alto	Tratar
R04	Adulte-ração de dados	Não observância da Norma de Acesso e Tratamento da Informação e/ou do Processo de Gestão de Dados de Pesquisa e/ou Política de Governança de Dados, Informação e Conhecimento da Embrapa; ausência de controle de acesso aos sistemas e aos repositórios de dados; falta de treinamento e conscientização sobre segurança da informação, atitude antiética ou delituosa.	Impossibilidade de recuperação dos dados, reúso e compartilhamento; prejuízo à imagem da Empresa; prejuízo financeiro e científico.	Norma de Acesso e Tratamento da Informação; Processo de Gestão de Dados de Pesquisa; Código de Conduta, Ética e Integridade da Embrapa; Norma de Uso de Dados para Negócios da Embrapa; Política de Governança de Dados, Informação e Conhecimento da Embrapa; contrato individual de trabalho.	Média	Alto	Alto	Tratar

Prevenção

Todos os empregados e colaboradores da Embrapa devem receber treinamentos sobre práticas seguras de manipulação e armazenamento de dados, além de serem conscientizados quanto ao seu papel no contexto da SI.

O acesso aos sistemas e aos repositórios de dados de PD&I deve ser controlado por meio da autenticação do usuário mediante o uso de senha, *token*, biometria ou outro dispositivo de segurança que garanta a identificação do usuário e o nível de acesso a ele atribuído.

Todos os sistemas operacionais, aplicativos e softwares de segurança devem ser regularmente atualizados com as últimas versões e *patches* de segurança, de forma a mitigar vulnerabilidades conhecidas e proteger os dados de PD&I contra ameaças cibernéticas.

Os sistemas e os repositórios de dados de PD&I devem estar incluídos nas políticas de backup definidas pelas respectivas áreas de suporte de TIC, como forma de garantir a recuperação dos dados diante de algum incidente que provoque sua perda.

Toda proposta de projeto de pesquisa submetida ao Sistema de Gestão da Programação (Sistema Embrapa de Gestão – SEG) deve conter o Plano de Gestão de Dados, disponível no sistema Ideare, o qual contempla informações sobre:

- Caracterização dos dados.
- Armazenamento, segurança e preservação dos dados
- Acesso e compartilhamento dos dados.

Os dados brutos (informações de contexto da coleta e metadados) e os dados resultantes dos projetos de PD&I produzidos e coletados pela Embrapa, inclusive em parceria, devem estar de acordo com o Plano de Gestão de Dados e armazenados nos sistemas e/ou repositórios corporativos, de acordo com a área do conhecimento, natureza dos dados e normativos específicos. Esses dados devem ser facilmente recuperáveis, acessíveis, interoperáveis e reutilizáveis, respeitando-se os níveis de proteção que lhes forem atribuídos.

Dados de PD&I cujo sigilo seja imprescindível à segurança da sociedade e do Estado, art. 7º, § 1º da Lei nº 12.527 (Brasil, 2011), Lei de Acesso à Informação (LAI), bem como os dados que recaiam sobre outras hipóteses de sigilo legal, seja comercial, industrial, de propriedade intelectual, parcerias, entre outros, devem ter seu acesso restrito a empregados que tenham necessidade de conhecer seu conteúdo por força de atribuição funcional (grupo de acesso), não sendo necessária a classificação em grau de sigilo. Caso esses dados não se enquadrem nos critérios de sigilo citados, estarão sujeitos à

disponibilização à sociedade como "dados abertos", em apoio às ações de transparência ativa da Embrapa e aos movimentos globais de Ciência Aberta e Governo Aberto.

> A restrição de acesso do público externo aos dados de PD&I, produzidos pela Embrapa, deve perdurar pelo período que for necessário à consecução do projeto ou até que a divulgação das informações não possibilite vantagem de qualquer natureza a outra nação, empresa ou grupo de interesse externo; nem risco algum à segurança da sociedade e do Estado.
>
> A restrição de acesso do público interno da Embrapa aos dados de PD&I, produzidos no âmbito da Empresa, deve ser mantida por no máximo 2 anos após o término do projeto, ou conforme termos estabelecidos em acordos de cooperação, contrato ou outro instrumento jurídico (Embrapa, 2020, p. 62).

Dados de PD&I poderão ser reutilizados em novos contextos, estudos e projetos, desde que garantido o devido reconhecimento e crédito de autoria, observado o disposto na Lei nº 9.610/1998 (Brasil, 1998) e direitos relativos à propriedade industrial previstos na Lei nº 9.279/1996 (Brasil, 1996).

Os dados de PD&I armazenados nos sistemas e/ou repositórios devem estar submetidos às políticas de backups definidas pela área de Tecnologia da Informação da Embrapa, responsável pela manutenção desses dados.

Os dados de PD&I depositados e/ou consultados no Repositório de Dados de Pesquisa da Embrapa (Redape) devem ser precedidos da aceitação do Termo de Uso (CC BY-NC 4.0).

O compartilhamento de dados de PD&I não deve ocorrer via e-mails, mensagens de aplicativos ou, até mesmo, chamadas telefônicas. Sempre que possível, deve-se optar por canais que ofereçam níveis adequados de segurança aos dados, garantindo que apenas o destinatário tenha acesso a eles.

As áreas de SI e de Gestão de Pessoas da Embrapa devem disponibilizar, para todos os empregados, treinamentos regulares sobre boas práticas de SI, como o uso adequado dos sistemas, a importância das senhas fortes e o reconhecimento de possíveis ameaças. Adicionalmente, devem incentivar uma cultura organizacional que valorize a SI e encoraje os empregados a relatar qualquer incidente ou comportamento suspeito.

Detecção

A comunicação inicial de um incidente de segurança envolvendo dados de PD&I pode ser feita por qualquer fonte ou pessoa interna ou externa à Embrapa. A comunicação por via diversa daquela diretamente ligada ao responsável pelo processo ou sistema afetado, em hipótese alguma, será considerada como motivo para seu não conhecimento.

O monitoramento sobre os dados de PD&I se inicia na fase de submissão das propostas de projeto, quando o Comitê Técnico Interno (CTI) deve exigir a elaboração do Plano de Gestão de Dados para aprovação do projeto.

Durante a execução do projeto de PD&I, a equipe do projeto deve fazer o monitoramento rotineiro da guarda e segurança dos dados e comunicar às áreas responsáveis todo e qualquer incidente de segurança que ocorrer.

Após a finalização do projeto, o CTI deve se certificar de que os dados gerados estão armazenados nos sistemas/repositórios corporativos em consonância com o Plano de Gestão de Dados do projeto. Caso isso não tenha ocorrido, o CTI deve orientar a equipe do projeto para que ela efetue o depósito dos dados.

A Supervisão de Inteligência em PD&I deve fazer o acompanhamento do Indicador de Gestão de Dados de Pesquisa, o qual avalia o nível efetivo de depósito de dados de PD&I nos sistemas/repositórios corporativos.

Tratamento

Uma vez detectado um incidente de perda, vazamento ou inacessibilidade de dados de PD&I, esse incidente deve ser tratado e analisado para que sejam, na medida do possível, preservadas todas as evidências do incidente, possibilitando posteriormente o rastreamento e identificação de suas causas.

O tratamento e a análise do incidente devem ser realizados observando-se a definição dos seguintes atributos:

- Unidade e setor onde ocorreu o incidente.
- E-mail, telefone ou outro contato disponível do informante do incidente.
- Data e horário que incidente foi identificado.
- Descrição e consequência do incidente.
- Ativo afetado pelo incidente.
- Dados de PD&I afetados.
- Responsável pelo ativo afetado.
- Criticidade do incidente.

Resposta

A partir da confirmação de um incidente de perda, vazamento ou inacessibilidade de dados de PD&I, deve ser feita uma rápida avaliação do risco de propagação da ameaça que

o causou, bem como agir para que a ameaça não se propague e executar as seguintes ações:

- Restabelecer os serviços afetados no menor tempo possível.
- Atualizar sistemas operacionais, softwares antivírus e todos os outros ativos de TIC, quando o incidente for de natureza cibernética.
- Recuperar os dados a partir das cópias backups dos sistemas e repositórios de dados de PD&I ou de publicações que contenham os dados perdidos; ou, ainda, de mídias alternativas que eventualmente tenham sido utilizadas para a guarda dos dados.
- Apurar as responsabilidades de acordo com as leis, normas vigentes e os termos de compromisso e confidencialidade firmados pelo agente causador do incidente, quando o incidente for causado por ação ou inação humana.
- Buscar a proibição da utilização por terceiros dos dados vazados utilizando-se os preceitos dos direitos de propriedade intelectual e autoral.

Pós-incidente

Após a resposta ao incidente, deve ser agendada uma reunião de lições aprendidas entre os envolvidos nos processos afetados pelo incidente e a área responsável pela SI na Embrapa, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos, inclusive deste PSI.

DADOS PESSOAIS

Escândalos de vazamentos de dados pessoais tornaram-se comuns nos dias atuais, principalmente pela utilização, cada vez mais massiva, dos recursos cibernéticos. A Embrapa tem feito esforços no intuito de se adequar à Lei Geral de Proteção de Dados (LGPD) e garantir a segurança dos dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento no âmbito da Empresa.

Matriz de riscos

Esta seção apresenta a matriz de riscos resultante do processo de análise de riscos realizado para identificar, avaliar e priorizar potenciais ameaças relacionadas ao tema de dados pessoais (Tabela 3). A matriz foi elaborada com base na Metodologia de Gestão de Riscos Corporativos da Embrapa (Embrapa, 2025).

Tabela 3. Matriz de riscos para segurança de dados pessoais.

Processo	Gestão de Dados Pessoais
Objetivo	Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
Ativo	Dados Pessoais

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Perda de dados	Não observância à Lei Geral de Proteção de Dados Pessoais – LGPD – Lei nº 13.709/2018 (Brasil, 2018); não observância da Norma de Acesso e Tratamento da Informação e/ou da Política de Governança de Dados, Informação e Conhecimento da Embrapa; falta de preparo da equipe em relação à segurança de dados; desastres naturais.	Impossibilidade de recuperação dos dados, reúso e compartilhamento; prejuízo à imagem da Empresa; prejuízo financeiro e científico.	Lei Geral de Proteção de Dados Pessoais – LGPD – Lei nº 13.709/2018 (Brasil, 2018); Norma de Acesso e Tratamento da Informação; Política de Governança de Dados, Informação e Conhecimento da Embrapa; melhores práticas de procedimentos de backup.	Média	Alto	Alto	Tratar
R02	Vazamento de dados	Não observância à Lei Geral de Proteção de Dados Pessoais – LGPD – Lei nº 13.709/2018 (Brasil, 2018); não observância da Norma de Acesso e Tratamento da Informação e/ou da Política de Governança de Dados, Informação e Conhecimento da Embrapa; falta de preparo da equipe em relação à segurança de dados; desastres naturais.	Perda de oportunidades científicas, patentes, direito autoral e soberania nacional; desgaste e descredibilidade da imagem e marca da Empresa; divulgação indevida de dados por terceiros.	Lei Geral de Proteção de Dados Pessoais – LGPD – Lei nº 13.709/2018 (Brasil, 2018); Norma de Acesso e Tratamento da Informação; Código de Conduta, Ética e Integridade da Embrapa; Norma de Uso de Dados para Negócios da Embrapa; Política de Governança de Dados, Informação e Conhecimento da Embrapa; política/cartilha/treinamento de segurança da informação.	Média	Alto	Alto	Tratar

Prevenção

Todos os empregados e colaboradores da Embrapa devem receber treinamentos sobre práticas seguras de manipulação e armazenamento de dados, além de serem conscientizados quanto ao seu papel no contexto da SI.

O acesso aos sistemas e aos repositórios de dados deve ser controlado por meio da autenticação do usuário mediante o uso de senha, *token*, biometria ou outro dispositivo de segurança que garanta a identificação do usuário e o nível de acesso a ele atribuído.

Todos os sistemas operacionais, aplicativos e softwares de segurança devem ser regularmente atualizados com as últimas versões e *patches* de segurança, de forma a mitigar vulnerabilidades conhecidas e proteger os dados pessoais contra ameaças cibernéticas.

Os sistemas e os repositórios que lidam com dados pessoais devem estar incluídos nas políticas de backup definidas pelas respectivas áreas de suporte de TIC, como forma de garantir a recuperação dos dados diante de algum incidente que provoque sua perda.

As áreas de SI e de Gestão de Pessoas da Embrapa devem disponibilizar, para todos os empregados, treinamentos regulares sobre boas práticas de SI, como o uso adequado dos sistemas, a importância das senhas fortes e o reconhecimento de possíveis ameaças. Adicionalmente, devem incentivar uma cultura organizacional que valorize a SI e encoraje os empregados a relatar qualquer incidente ou comportamento suspeito.

Detecção

A comunicação inicial de um incidente de segurança envolvendo dados pessoais pode ser feita por qualquer fonte ou pessoa interna ou externa à Embrapa. A comunicação por via diversa daquela diretamente ao responsável pelo processo ou sistema afetado, em hipótese alguma, será considerada como motivo para seu não conhecimento.

A comunicação deve ser feita ao encarregado pelo Tratamento de Dados Pessoais.

Conforme art. 48, da Lei Geral de Proteção de Dados (Brasil, 2018), caso a ocorrência de incidente de segurança possa acarretar risco ou dano relevante aos titulares, esta ocorrência deverá ser comunicada à Autoridade Nacional de Proteção de Dados (ANPD) pelo encarregado de dados. A mensagem será desenvolvida pela área de negócio, com assistência e orientação do encarregado e com suporte do jurídico mencionando, no mínimo:

- A descrição da natureza dos dados pessoais afetados.
- As informações sobre os titulares envolvidos.

- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial.
- Os riscos relacionados ao incidente.
- Os motivos da morosidade, no caso de a comunicação não ter sido imediata.
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Tratamento

Uma vez detectado um incidente de SI envolvendo dados pessoais, ele deve ser tratado e analisado para que sejam, na medida do possível, preservadas todas as evidências do incidente, possibilitando posteriormente o rastreamento e identificação de suas causas.

O tratamento e a análise do incidente devem ser realizados observando-se a definição dos seguintes atributos:

- Unidade e setor onde ocorreu o incidente.
- E-mail, telefone ou outro contato disponível do informante do incidente.
- Data e horário que o incidente foi identificado.
- Descrição e consequência do incidente.
- Quantidade de titulares de dados afetados.
- Ativo afetado pelo incidente.
- Responsável pelo ativo afetado.
- Criticidade do incidente.

Resposta

A partir da confirmação de um incidente de SI envolvendo dados pessoais, deve ser feita uma rápida avaliação do risco de propagação da ameaça que o causou, bem como agir para que a ameaça não se propague e executar as seguintes ações:

- Restabelecer os serviços afetados no menor tempo possível.
- Atualizar sistemas operacionais, softwares antivírus e todos os outros ativos de TIC, quando o incidente for de natureza cibernética.

- Recuperar os dados pessoais a partir das cópias backups dos sistemas e repositórios ou de publicações que contenham os dados perdidos; ou, ainda, de mídias alternativas que eventualmente tenham sido utilizadas para a guarda dos dados.
- Apurar as responsabilidades de acordo com a LGPD, normas vigentes e os termos de compromisso e confidencialidade firmados pelo agente causador do incidente quando o incidente for causado por ação ou inação humana.

Pós-incidente

Após a resposta ao incidente, deve ser agendada uma reunião de lições aprendidas entre os envolvidos nos processos afetados pelo incidente e a área responsável pela SI na Embrapa, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos — inclusive deste PSI.

DOCUMENTOS

Os documentos são a principal forma de registro, representação e apresentação da informação. Eles podem ser físicos ou eletrônicos, contendo a representação de informações nos formatos de texto, áudio ou imagem. Estabelecer procedimentos para produção, nível de acesso e utilização, eliminação, descarte ou arquivamento dos documentos é primordial para assegurar a SI.

Matriz de riscos

Esta seção apresenta a matriz de riscos resultante do processo de análise de riscos realizado para identificar, avaliar e priorizar potenciais ameaças relacionadas ao tema documentos (Tabela 4). A matriz foi elaborada com base na Metodologia de Gestão de Riscos Corporativos da Embrapa (Embrapa, 2025).

Tabela 4. Matriz de riscos para gestão de documentos.

Processo	Gestão Documental Arquivística
Objetivo	Possibilitar à Embrapa a gestão documental e a proteção especial a documentos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.
Ativo	Documentos arquivísticos e bibliográficos

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Acesso e divulgação indevidos a informações pessoais sigilosas ou restritas, e a informações estratégicas (inclusive propriedade intelectual)	Não observância do controle de acesso devido; registro em locais não apropriados e sem a observância do controle de acesso devido; falta de definição objetiva dos critérios de restrição de acesso a serem adotados; ausência de um processo de classificação da informação ou falhas de implementação; ausência de capacitações e campanhas de sensibilização em proteção de informações sensíveis.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico; prejudicar ou causar risco a planos ou operações estratégicos.	Norma de Acesso e Tratamento da Informação; Norma de Gestão Documental Arquivística e Uso do Sistema Eletrônico de Informações (SEI); Manual de Gestão Documental Arquivística.	Média	Alto	Alto	Tratar
R02	Perda ou adulteração de informações em documentos eletrônicos	Obsolescência de mídias digitais; extinção/desativação de sistema eletrônico; falha no processo ou no sistema de backup; controles de integridades inadequados.	Prejuízo à imagem da Embrapa; prejuízo financeiro; responder a processos judiciais e de fiscalização e controle; prejuízo à imagem da Embrapa.	Norma de Acesso e Tratamento da Informação; Norma de Acesso e Tratamento da Informação; Norma de Gestão Documental Arquivística e Uso do Sistema Eletrônico de Informações (SEI); Manual de Gestão Documental Arquivística.	Média	Alto	Alto	Tratar
R03	Perda ou destruição de documentos físicos	Não observância dos procedimentos descritos no Manual de Gestão Documental Arquivística.	Prejuízo à imagem da Embrapa; prejuízo à memória institucional; prejuízo financeiro; responder a processos judiciais e de fiscalização e controle; prejuízo à imagem da Embrapa.	Norma de Acesso e Tratamento da Informação; Norma de Gestão Documental Arquivística e Uso do Sistema Eletrônico de Informações (SEI); Manual de Gestão Documental Arquivística.	Média	Alto	Alto	Tratar
R04	Acesso e divulgação indevida de informações técnico-científicas	Registro no Repositório de Informação Tecnológica da Embrapa (Ainfo) sem a observância do controle devido.	Responder a processos judiciais referentes a direito autoral; prejuízo financeiro; prejuízo à imagem da Embrapa.	Documento Manual dos Indicadores de Produção Técnico-Científica: orientações para registro no Ainfo.	Média	Alto	Alto	Tratar

Prevenção

A prática de atos administrativos deverá ser realizada por meio do Sistema Eletrônico de Informações (SEI). Tal prática obedecerá aos princípios constitucionais da legalidade, da impessoalidade, da moralidade, da publicidade e da eficiência, sem prejuízo dos demais princípios norteadores da Administração Pública Federal, cabendo aos usuários do SEI manter absoluta discrição com relação às informações neles contidas, conforme a correspondente categoria de acesso.

Ao receber e/ou registrar documentos no SEI, deve ser feito o uso da marcação de nível de acesso ao processo condizente com teor da informação e adotar os procedimentos descritos no Manual de Gestão Documental Arquivística.

No momento da produção do documento e ao longo do seu ciclo de vida, devem ser criados metadados, tais como aqueles que visam:

- Identificar a ação ou atividade que o documento registra (assunto).
- Identificar a unidade administrativa à qual o documento pertence (produtor).
- Identificar e registrar/atribuir o grau de sigilo ou outras restrições legais de acesso.

O documento com marcação de sigilo será encaminhado ao destinatário sem ser aberto, cabendo-lhe sua digitalização, seu registro e o respectivo tratamento da informação, conforme o grau de sigilo aplicável. Havendo indícios de violação de correspondência oficial recebida, o empregado que identificar o fato deverá registrar no ato de recebimento, bem como comunicá-lo imediatamente à autoridade competente.

O registro de documentos em sistemas oficiais deverá ser precedido da marcação do nível de acesso de forma a proteger as informações. Deve-se observar o nível de acesso do documento: a) público; b) restrito ou c) sigiloso.

A definição do nível de acesso sigiloso deve ocorrer apenas nos casos previstos em legislação. O registro de um documento como sigiloso implica a necessidade de controle especial de acesso limitado à pessoa autorizada a acessá-lo.

A classificação de documentos quanto ao grau de sigilo e a possibilidade de limitação do acesso aos empregados autorizados e aos interessados no processo observarão os termos da Lei nº 12.527/2011 (Brasil, 2011) e da norma de Acesso e Tratamento da Informação da Embrapa (Embrapa, 2020).

Os critérios para marcação de acesso a documentos devem ser objetivos, e as classificações de acesso devem ser revisadas periodicamente, a fim de garantir sua atualização, de modo a restringir e garantir que somente os indivíduos autorizados tenham acesso aos documentos classificados e aos originalmente sigilosos.

Os responsáveis pelo registro de documentos em sistemas oficiais deverão, no ato do registro, ou a qualquer momento, sinalizar o nível de acesso da informação, sob pena de responderem diretamente pelos danos causados em decorrência da divulgação não autorizada ou da utilização indevida de informações sigilosas ou informações pessoais.

Os sistemas ou repositórios devem possuir controles de acesso adequados, como identificação da permissão de acesso dos usuários. Documentos de acesso restrito e/ou sigiloso não podem ser registrados em sistemas que não contenham medidas de segurança necessárias à proteção da informação.

Deve ser mantido o registro de acesso em trilha de auditoria, onde conste todos os acessos, tentativas de acesso e uso dos documentos (visualização, impressão, transmissão e cópia para a área de transferência), com identificação de usuário, data, hora e, se possível, estação de trabalho.

As solicitações de acesso a processo e documentos registrados em sistemas oficiais seguirão o disposto na Lei nº 12.527/2011 (Brasil, 2011) e em regulamentação aplicável. Os documentos sigilosos em meio físico deverão ser encaminhados para guarda no Arquivo, geral ou central, em mobiliário que assegure a sua proteção de acesso indevido.

O arquivamento de mídias e documentos relativos a processos concluídos nas Unidades Centrais (UCs) e que contenham informação restrita ou sigilosa será feito no Arquivo Central da Embrapa. Os documentos que envolvem dados pessoais sigilosos serão depositados apenas em sistemas oficiais e que possuam controle de acesso conforme estabelecido nos normativos vigentes.

Todas Unidades da Embrapa devem providenciar áreas apropriadas para a instalação de seu Arquivo Geral. A área destinada à guarda dos acervos documentais arquivísticos deve garantir sua segurança e preservação, bem como se basear no tamanho e característica do acervo (textual, audiovisual, fotográfico, etc.), conforme orientações constantes do Manual de Gestão Documental Arquivística da Embrapa.

O armazenamento de documentos digitais deve ser feito em dispositivos de memória não voláteis que garantam o armazenamento adequado para documentos de valor permanente.

O armazenamento deve garantir a autenticidade e o acesso aos documentos pelo tempo estipulado na tabela de temporalidade e destinação da Embrapa conforme norma Gestão Documental Arquivística e Uso do Sistema Eletrônico de Informações (SEI) (Embrapa, 2021). Documentos de valor permanente, independentemente do formato, requerem um armazenamento criterioso desde o momento da sua produção, para garantir sua preservação em longo prazo.

Para garantir sua interoperabilidade, os documentos eletrônicos devem utilizar software e hardware que sejam interoperáveis e não sejam produzidos em formatos proprietários.

Deve ser feito o monitoramento contínuo de hardware e software para detectar obsolescência de formatos, suportes e padrões, bem como implementar procedimentos de preservação.

Para evitar a eliminação indevida de documentos, estes somente poderão ser eliminados depois de concluído o processo de avaliação e seleção, conforme descrito no Manual de Gestão Documental Arquivística da Embrapa.

A eliminação de documentos de arquivo da Embrapa só deverá ocorrer se o prazo de guarda desses documentos estiver previsto na tabela de temporalidade e quando devidamente aprovada pela autoridade competente na esfera de atuação, respeitado o disposto no art. 9° da Lei n° 8.159, de 8 de janeiro de 1991 (Brasil, 1991), e na Resolução nº 44, de 14 de fevereiro de 2020 (Brasil, 2020), que define o processo de eliminação no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (Sinar) do Conselho Nacional de Arquivos (Conarq).

Detecção

Constatada a perda de documento, a autoridade competente deve ser comunicada, cabendo a ela promover a apuração dos fatos, por meio do procedimento apuratório cabível, e designar, formalmente, um empregado ou uma comissão para proceder à reconstituição do processo.

A comunicação inicial de um incidente de SI deve ser feita por qualquer fonte ou pessoa interna ou externa à Embrapa. A comunicação realizada por via diferente daquela diretamente ligada ao responsável pelo processo ou sistema afetado, em hipótese alguma, poderá ser utilizada como motivo para alegar desconhecimento do incidente.

Os gestores das áreas que mantêm a guarda de documentos devem manter mecanismos de controle de acesso e guarda que permitam a detecção de acessos indevidos ou a iminência de perda de documentos.

Constatado o acesso indevido a documento restrito ou sigiloso, deverão ser adotados os meios necessários para restringir novos acessos, realizando-se a marcação de restrição e os procedimentos de proteção compatíveis com a restrição. A autoridade competente deverá ser comunicada, cabendo a ela promover a apuração dos fatos e a adoção das medidas cabíveis.

Tratamento

Uma vez detectado um incidente de SI envolvendo documento restrito ou sigiloso, esse incidente deve ser tratado e analisado para que sejam, na medida do possível, preservadas todas as evidências do incidente, possibilitando posteriormente o rastreamento e a identificação de suas causas.

No caso de acesso indevido, deve-se restringir o acesso assim que tomar conhecimento, bem como comunicar à autoridade competente para adoção de ações pertinentes.

Ao identificar o registro de um documento de acesso restrito em "ambiente" inadequado, deve-se realizar a retirada imediata de tal documento e comunicar à autoridade competente para adoção das ações cabíveis.

Ao identificar a divulgação de documento/informação de acesso restrito, deve-se comunicar à autoridade competente para adoção das ações cabíveis.

O tratamento e a análise do incidente devem ser realizados observando-se a definição dos seguintes atributos:

- Unidade e setor onde ocorreu o incidente.
- E-mail, telefone ou outro contato disponível do informante do incidente.
- Data e horário que incidente foi identificado.
- Descrição e consequência do incidente.
- Quantidade de documentos afetados.
- Ativo de informação afetado pelo incidente.
- Responsável pelo ativo de informação afetado.
- Criticidade do incidente.

Resposta

A partir da confirmação de um incidente de SI envolvendo documentos, deve ser feita uma rápida avaliação do risco de propagação da ameaça que o causou, bem como agir para que a ameaça não se propague e executar as seguintes ações:

- Comunicar o incidente à autoridade competente no âmbito da Unidade para que os fatos sejam apurados.
- Tomar as providências legais e administrativas cabíveis, quando constatada a má-fé na atuação do agente causador do incidente, pela autoridade competente.

- Inserir uma declaração de retificação de documento excluído/cancelado informando a ocorrência do erro e que o documento será substituído por outro de mesmo teor ou com conteúdo similar, no caso de documento excluído ou cancelado que não seja possível sua recuperação.
- Atualizar sistemas operacionais, softwares antivírus e todos os outros ativos de TIC quando o incidente for de natureza cibernética.

Pós-incidente

Após a resposta ao incidente, deve ser agendada uma reunião de lições aprendidas entre os envolvidos nos processos afetados pelo incidente, a área responsável pela SI na Embrapa e a área responsável pela gestão de documentos e informações, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos — inclusive deste PSI.

INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

À medida que avançou a utilização da tecnologia da informação e comunicação (TIC) para as mais variadas atividades organizacionais, inclusive para prestação de serviços, pesquisa e processos de negócio de uma forma geral, cresceram também as ameaças cibernéticas que colocam em risco a administração das empresas e da própria sociedade. Desse modo, proteger o espaço cibernético utilizado pela Embrapa requer visão atenta, liderança e apoio efetivo da alta gestão.

Matriz de riscos

Esta seção apresenta a matriz de riscos resultante do processo de análise de riscos realizado para identificar, avaliar e priorizar potenciais ameaças relacionadas ao tema tecnologia da informação e comunicação (Tabela 5). A matriz foi elaborada com base na Metodologia de Gestão de Riscos Corporativos da Embrapa (Embrapa, 2025).

Tabela 5. Matriz de riscos para Infraestrutura de tecnologia da informação e comunicação.

Processo	Tecnologia da Informação e Comunicações (TIC)
Objetivo	Efetuar a gestão dos recursos de tecnologia da informação (TI), alinhando-se a utilização dos recursos corporativos de tecnologia da informação e comunicação (TIC) às necessidades das áreas de negócio.
Ativo	Estrutura organizacional

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Incapacidade de gestão da segurança da informação (SI)	Desconhecimento da gestão com relação à importância e complexidade da segurança cibernética; desconhecimento das normas e boas práticas em SI, em especial as que tratam da Organização da Segurança da Informação; falta de comprometimento da gestão em relação à segurança cibernética.	Cobranças e sanções pelos órgãos de controle da Administração Pública; prejuízo à imagem da Empresa; prejuízo financeiro e científico; perda de credibilidade; falhas de segurança que comprometem a disponibilidade, integridade e confidencialidade dos dados e informações.	Política de Governança de Dados, Informação e Conhecimento, as normas de uso dos recursos de TI, os controles de segurança cibernética implantados na infraestrutura de TI, comitês e comissões instituídos, relacionados ao tema.	Alta	Alto	Alto	Tratar

Ativo	Redes

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Ataques e invasões à infraestrutura básica de redes	Ausência de um plano sistemático de atualizações/correções em sistemas e serviços; servidores e sistemas mal configurados ou desatualizados; capacitação insuficiente para trabalhar com determinadas tecnologias; ausência de varreduras regulares para identificar proativamente vulnerabilidades e falhas em sistemas.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Segurança do perímetro de rede, realizado por meio de firewall, IPS, antivírus e outros mecanismos de segurança; atualização automatizada de sistema operacional e aplicativos; Iniciativas de criação de inventário de ativos com informações sobre o ativo, responsável, configurações, etc.; sistema de alerta de indisponibilidade de serviços de infraestrutura; sistema de monitoramento de *logs* de acesso de sistemas e serviços.	Alta	Alto	Alto	Tratar
R02	Indisponibilidade	Ataques cibernéticos; desastres naturais; quedas de energia.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Sistema de alerta de indisponibilidade de serviços de infraestrutura; sistema de monitoramento de *logs* de acesso de sistemas e serviços; segurança do perímetro de rede, realizado por meio de firewall, IPS, antivírus e outros mecanismos de segurança; atualização automatizada de sistema operacional e aplicativos; sistema de para-raios; sistema de grupos geradores de energia.	Alta	Alto	Alto	Tratar

Continua...

Tabela 5. Continuação.

Ativo Sistemas operacionais

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Incompatibilidade com sistemas e servidores de aplicação	Ausência de um plano sistemático de atualizações/correções em sistemas e serviços; servidores e sistemas mal configurados ou desatualizados; capacitação insuficiente para trabalhar com determinadas tecnologias; falta de suporte técnico; ausência de varreduras regulares para identificar proativamente vulnerabilidades e falhas em sistemas.	Paralisação dos negócios da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico.	Atualização automatizada de sistema operacional e aplicativos; iniciativas de criação de inventário de ativos com informações sobre o ativo, responsável, configurações, etc.; sistema de alerta de indisponibilidade de serviços de infraestrutura; sistema de monitoramento de *logs* de acesso de sistemas e serviços.	Média	Alto	Alto	Tratar
R02	Obsolescência e travamentos	Ausência de um plano sistemático de atualizações/correções em sistemas e serviços; servidores e sistemas mal configurados ou desatualizados; capacitação insuficiente para trabalhar com determinadas tecnologias; falta de suporte técnico; ausência de varreduras regulares para identificar proativamente vulnerabilidades e falhas em sistemas.	Paralisação dos negócios da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico.	Atualização automatizada de sistema operacional e aplicativos; iniciativas de criação de inventário de ativos com informações sobre o ativo, responsável, configurações, etc.; sistema de alerta de indisponibilidade de serviços de infraestrutura; sistema de monitoramento de logs de acesso de sistemas e serviços.	Média	Alto	Alto	Tratar

Ativo Documentos eletrônicos

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Perda ou adulteração de informações em documentos eletrônicos; acesso e divulgação indevida de informações técnico-científicas.	Credenciais de acesso descobertas e utilizadas por terceiros ou roubadas; a informação de desligamento de empregados ou da função não é repassada à área de TI para remoção dos direitos de acesso; ausência de auditorias que avaliem as permissões em sistemas e aplicativos; ausência ou ineficácia de procedimentos de backup.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Procedimentos de backup para sistemas, base de dados, código-fonte de programas e configurações de sistemas e serviços; mecanismos de controle de acesso, software de proteção contra malwares; software de criptografia para proteger as informações confidenciais armazenadas nos dispositivos de armazenamento de dados e informações.	Média	Alto	Alto	Tratar

Continua...

Tabela 5. Continuação.

Ativo	Servidores (Hardware)

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Invasão por *hackers*	Ausência de um plano sistemático de atualizações/correções em sistemas operacionais e serviços; servidores e sistemas mal configurados ou desatualizados; capacitação insuficiente para trabalhar com determinadas tecnologias; ausência de varreduras regulares para identificar proativamente vulnerabilidades e falhas em redes e sistemas; ausência de sistemas de controle de acesso.	Prejuízo à imagem da Embrapa; perda de credibilidade; paralisação dos negócios; prejuízo financeiro; prejuízo científico e tecnológico.	Segurança do perímetro de rede, realizado por meio de firewall, IPS, antivírus e outros mecanismos de segurança; atualização automatizada de sistema operacional e aplicativos; iniciativas de criação de inventário de ativos com informações sobre o ativo, responsável, configurações, etc.; sistema de alerta de indisponibilidade de serviços de infraestrutura; sistema de monitoramento de *logs* de acesso de sistemas e serviços.	Média	Alto	Alto	Tratar
R02	Indisponibilidade	Ataques cibernéticos; desastres naturais; quedas de energia.	Prejuízo à imagem da Embrapa; perda de credibilidade; paralisação dos negócios; prejuízo financeiro; prejuízo científico e tecnológico.	Segurança do perímetro de rede, realizado por meio de firewall, IPS, antivírus e outros mecanismos de segurança; atualização automatizada de sistema operacional e aplicativos; iniciativas de criação de inventário de ativos com informações sobre o ativo, responsável, configurações, etc.; sistema de alerta de indisponibilidade de serviços de infraestrutura; sistema de monitoramento de *logs* de acesso de sistemas e serviços; sistema de para-raios; sistema de grupos geradores de energia.	Média	Alto	Alto	Tratar

Ativo	Instalações físicas

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Acesso indevido a áreas restritas ao acesso público (*datacenter*, laboratórios, campos experimentais, etc.).	Ausência de controles adequados para limitar o acesso a áreas restritas da Empresa; ausência de campanhas sistemáticas que promovam uma cultura de segurança.	Danos a equipamentos, vazamento de dados, riscos à segurança das informações e aos empregados.	Controle de entrada com identificação de visitantes nas portarias; controle de acesso ao *datacenter* e laboratórios com o uso de câmeras de vídeo e, em alguns casos, trancas com o uso de biometria.	Média	Alto	Alto	Tratar

Continua...

Tabela 5. Continuação.

Ativo	Dados

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Perda de dados	Ausência ou ineficácia de uma política de backup; credenciais de acesso a sistemas e repositórios de dados, descobertas e utilizadas por terceiros ou roubadas; ausência de auditorias que avaliem as permissões em sistemas e aplicativos; desastres naturais.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Procedimentos de backup para sistemas, base de dados, código-fonte de programas e configurações de sistemas e serviços; mecanismos de controle de acesso, software de proteção contra malwares; software de criptografia para proteger as informações confidenciais armazenadas nos dispositivos de armazenamento de dados e informações.	Média	Alto	Alto	Tratar (mitigar)
R02	Vazamento de dados	Credenciais de acesso a sistemas e repositórios de dados, descobertas e utilizadas por terceiros ou roubadas; ausência de auditorias que avaliem as permissões em sistemas e aplicativos.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Procedimentos de backup para sistemas, base de dados, código fonte de programas e configurações de sistemas e serviços; mecanismos de controle de acesso, software de proteção contra malwares; software de criptografia para proteger as informações confidenciais armazenadas nos dispositivos de armazenamento de dados e informações.	Média	Alto	Alto	Tratar
R03	Indisponibilidade de dados	Ataques cibernéticos; Indisponibilidade de redes; desastres naturais.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Segurança do perímetro de rede, realizado por meio de Firewall, IPS, antivírus e outros mecanismos de segurança; atualização automatizada de sistema operacional e aplicativos (Windows Update e Satellite); sistema de alerta de indisponibilidade de serviços de infraestrutura; sistema de para-raios; sistema de grupos geradores de energia.	Média	Alto	Alto	Tratar

Continua...

Tabela 5. Continuação.

Ativo Sistemas de informação

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Indisponibilidade	Ataques cibernéticos; indisponibilidade de redes; desastres naturais.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico.	Segurança do perímetro de rede, realizado por meio de firewall, IPS, antivírus e outros mecanismos de segurança; atualização automatizada de sistema operacional e aplicativos; sistema de alerta de indisponibilidade de serviços de infraestrutura; sistema de para-raios; sistema de grupos geradores de energia.	Média	Alto	Alto	Tratar
R02	Funcionamento anormal	Erros no levantamento de requisitos do sistema; erros na codificação do sistema; ataques cibernéticos.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Metodologias padronizadas para o desenvolvimento de software; separação dos ambientes de produção, homologação e desenvolvimento de sistemas; separação dos sistemas de *back-end* (servidor de aplicação e banco de dados) da interface do usuário (*front-end*) através de zonas com diferentes controles e requisitos de segurança; uso de software de segurança (IPS) para identificação e bloqueio automático de vulnerabilidades em sistemas e serviços; uso de firewall para controlar os tráfegos entre as diferentes zonas de segurança; uso de criptografia ponto a ponto nas comunicações entre o usuário e os serviços Web e VPN *Secure Socket Layer* (SSL) ou *Transport Layer Security* (TLS).	Média	Alto	Alto	Tratar

Ativo Equipamentos fixos e móveis (Desktops, notebooks, tablets, smartphones, etc.)

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Vazamento de informações sensíveis	Sistema operacional desatualizado, mal configurado, sem proteção de antivírus; conscientização/capacitação insuficientes para utilizar os recursos de TI com segurança; extravio ou perda de dispositivos móveis.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Inventário de hardware e software para estações de trabalho e notebooks; sistema antivírus com atualização automática; Norma de Teletrabalho; melhores práticas de procedimentos de backup.	Média	Alto	Alto	Tratar
R02	Perda de dados	Sistema operacional desatualizado, mal configurado, sem proteção de antivírus; conscientização/capacitação insuficientes para utilizar os recursos de TI com segurança; extravio ou perda de dispositivos móveis; compartilhamento do equipamento com pessoas não autorizadas.	Prejuízo à imagem da Embrapa; prejuízo financeiro; prejuízo científico e tecnológico; prejuízo à soberania nacional.	Inventário de hardware e software para estações de trabalho e notebooks; sistema antivírus com atualização automática; Norma de Teletrabalho; melhores práticas de procedimentos de backup.	Média	Alto	Alto	Tratar

Prevenção

O acesso aos espaços físicos das Unidades da Embrapa e da Sede devem ser controlados com a identificação de visitantes, uso de etiquetas de identificação ou crachá com tecnologia que permita o rastreio do visitante em áreas críticas da Embrapa.

O controle de acesso aos *datacenters* e laboratórios deve ser feito com o uso de câmeras de monitoramento e trancas com o uso de biometria e crachás magnéticos.

O acesso à informação, seus recursos de processamento e os processos críticos de negócio devem ser controlados e criteriosamente autorizados para uso.

Devem ser utilizados controles de autenticação rigorosos, em determinados casos, com uso de um segundo fator de autenticação, para que apenas usuários autorizados possam obter acesso a dados e sistemas da Embrapa.

Devem ser utilizados controles de acesso do usuário de acordo com o princípio do menor privilégio, ou seja, o usuário deve ter acesso apenas ao que é absolutamente necessário ao desempenho de suas atribuições funcionais.

Devem ser utilizados controles para limitar o número de tentativas de login malsucedidas (por exemplo, após três tentativas de login o usuário pode ser forçado a aguardar um tempo determinado antes de fazer novas tentativas ou mesmo bloqueado).

O acesso remoto deve ser controlado, sendo o seu uso autorizado quando absolutamente necessário para o desempenho das funções do empregado, e, sempre que possível, deve-se utilizar mais de um fator de autenticação.

O processo de autorização e remoção de acessos deve ser automatizado por meio da integração com sistema de gestão de empregados.

Os controles devem ser capazes de restringir o acesso de acordo com as políticas definidas pelos proprietários dos sistemas, isto é, deve-se minimizar a necessidade de privilégios especiais, memorização das senhas sem a devida proteção, evitar o uso indevido de credenciais de acesso (por exemplo, usando autenticação forte, como cartões inteligentes, biometria ou *tokens*).

O desenvolvimento de software deve seguir processos e utilizar tecnologias que atendam a todos os requisitos de segurança necessários para garantir soluções que minimizem as vulnerabilidades do ambiente cibernético.

As Unidades da Embrapa — Unidades Centrais (UCs) e Descentralizadas (UDs) — e a Sede devem manter atualizado o inventário de sistemas críticos, com gestores responsáveis nomeados, contatos técnicos, configurações e backups realizados.

Da mesma forma, devem estabelecer padrões de configuração mínimos (*baseline*) para garantir a segurança de hardware, software, sistemas de autenticação e padrões de desenvolvimento de software.

As UCs e UDs e a Sede devem documentar e manter atualizada a topologia de rede, configurações de firewall, ativos de redes, sistemas e serviços.

As UCs e UDs a e a Sede devem adotar ferramentas de verificação de vulnerabilidades que possibilitem, se desejável, a correção automática. Para os demais casos, deve-se estabelecer um plano de correção manual e programada.

As Unidades da Embrapa e a Sede devem adotar tecnologias para a verificação de portas de rede/captura de pacotes, ferramentas inspeção/detecção de intrusão — proteção (IPS/IDS), monitoramento de *endpoints*, controle de acesso, análise da qualidade de senhas, criptografia, análise de *logs*, interrupção de comunicação de *botnet* de saída e configurações de firewalls.

Por fim, elas devem estabelecer procedimentos para aplicações de correções (*patches* de segurança) e atualizações de software.

As auditorias devem fornecer garantia de que os controles de segurança sejam aplicados corretamente. Da mesma forma, garantir que os controles sejam eficazes o suficiente para reduzir os riscos a níveis aceitáveis.

As áreas de SI juntamente com a área de Gestão de Pessoas devem realizar treinamento e conscientização sobre segurança, com o cuidado de adaptá-lo aos vários públicos. Entre os temas, devem ser incluídos o cuidado com as senhas, a proteção da área de trabalho, a política de mesa limpa, o uso da internet, a engenharia social, o compartilhamento de arquivos, malware nas redes sociais, os dados confidenciais, orientações e normativos vigentes sobre segurança da informação.

Os procedimentos de backup devem considerar a norma de classificação da informação (Embrapa, 2020), os critérios definidos pelo gestor e a legislação pertinente, realizados periodicamente, testados para garantir que as informações e os sistemas possam ser restaurados dentro dos prazos estabelecidos.

O procedimento de backup deve ser aprovada pelo gestor/proprietário do dado e obedecer aos planos de continuidade de negócios, bem como apoiada por obrigações legais, regulatórias e contratuais.

Os backups devem ser rotulados de forma clara e precisa, protegido contra modificação acidental e estar sujeito ao mesmo nível de proteção que as informações originais. Recomenda-se, ainda, que eles sejam mantidos por pelo menos três gerações do ciclo de backup, como recomendam as melhores práticas na área de tecnologia.

As cópias mantidas em meios de armazenamento, quando não mais necessárias, devem ser apropriadamente apagadas para garantir que informações sensíveis não saiam da Empresa, assim como a remoção de unidades de armazenamento de informações com grau de sigilo quando os computadores são enviados para manutenção fora da Empresa.

Detecção

A comunicação inicial de um incidente de segurança cibernética pode ser feita por qualquer fonte ou pessoa interna ou externa à Embrapa. A comunicação deve ser feita ao responsável pelo processo ou sistema afetado pelo incidente mediante e-mail, telefone ou qualquer outro meio possível.

Os métodos de detecção de intrusão devem ser apoiados por software especializado, como sistemas de detecção de intrusão de *host* (HIDS) e sistemas de detecção de intrusão de rede (NIDS, por exemplo o IPS). O software de detecção de intrusão deve ser atualizado automaticamente e dentro de prazos definidos (por exemplo, por meio de arquivos de assinatura de ataque). Os mecanismos de detecção de intrusão devem ser capazes de identificar:

- Acesso não autorizado a sistemas, dados e informações.
- Comportamento inesperado do usuário ou do aplicativo.
- Capacidade de fornecer relatórios gerenciais.
- Acesso que violem a política de segurança.
- Produção de alertas quando uma atividade suspeita for detectada (por exemplo, por meio de um console de gerenciamento, e-mail, mensagens de texto SMS, entre outros).

Os eventos detectados são analisados para compreender a natureza, os alvos e métodos de ataque. Na presença de um incidente, o seu tratamento é encaminhado pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (Etir) para a área responsável pelo tratamento e elaboração de relatórios. Os incidentes uma vez tratados devem ser analisados pela equipe de segurança, que pode relacioná-los com informações passadas, tendências de ataques, para avaliar uma possível reincidência ou desdobramentos que possam indicar um ataque com múltiplos alvos internos e externos à organização. A área de segurança deve elaborar relatórios mensais de eventos detectados e ações de mitigação tomadas.

Tratamento

Uma vez detectado um incidente de segurança cibernética, ele deve ser tratado e analisado para que sejam, na medida do possível, preservadas todas as evidências do incidente, possibilitando posteriormente o rastreamento e identificação de suas causas.

O tratamento e a análise do incidente devem ser realizados observando-se a definição dos seguintes atributos:

- Unidade e setor onde ocorreu o incidente.
- E-mail, telefone ou outro contato disponível do informante do incidente.
- Data e horário que o incidente foi identificado.
- Descrição e consequência do incidente.
- Ativos de informação afetados pelo incidente.
- Responsáveis pelos ativos afetados.
- Criticidade do incidente.

Resposta

A partir da confirmação de um incidente de segurança, deve ser feita uma rápida avaliação do risco de propagação da ameaça que o causou, bem como agir para que a ameaça não se propague e executar as seguintes ações:

- Comunicar o incidente à autoridade competente no âmbito da Unidade para que os fatos sejam apurados.
- Atualizar sistemas operacionais, softwares antivírus e todos os outros ativos de TIC.
- Encaminhar o incidente para a equipe executiva de resposta.
- Compartilhar as informações obtidas do processo de verificação de vulnerabilidades com as pessoas apropriadas para ajudar a eliminar vulnerabilidades semelhantes em outros sistemas de informação ou infraestruturas críticas.

Pós-incidente

Após a recuperação dos sistemas afetados pelo incidente de SI, devem ser realizados estudos para determinar a causa raiz e assim evitar que outras áreas de negócio ou Unidades de pesquisa sejam afetadas.

Se necessário, investigações forenses devem ser conduzidas para fins legais ou nos casos de comprometimentos de informações protegidas por grau de sigilo.

Os controles de segurança existentes devem ser examinados para determinar a necessidade de correções ou adequações.

Os detalhes do incidente de SI devem ser documentados em um relatório pós-incidente, com o objetivo de:

- Documentar o incidente, incluindo a causa, o impacto, as medidas de recuperação e as lições aprendidas.
- Compartilhar as lições aprendidas com outras áreas da Empresa para evitar que incidentes semelhantes se repitam.
- Melhorar os processos de segurança com base nas lições aprendidas com o incidente.

Deve ser realizada uma reunião de lições aprendidas entre os envolvidos nos processos afetados pelo incidente, a área responsável pela SI na Embrapa e a Etir, com o objetivo de discutir erros e dificuldades encontradas, bem como propor melhorias para os sistemas e processos.

INFRAESTRUTURA FÍSICA

A infraestrutura física permite acesso facilitado aos ativos de informação de uma organização, estando esses ativos mecanicamente depositados nessas estruturas ou, ainda, em outras que estejam a ela interconectadas por meios virtuais. A segurança da infraestrutura física para proteger os ativos de informação deve usar a abordagem de camadas ou linhas de defesa, que se iniciam com a proteção do perímetro do imóvel de forma adequada às condições ambientais e adjacentes.

Matriz de riscos

Esta seção apresenta a matriz de riscos resultante do processo de análise de riscos realizado para identificar, avaliar e priorizar potenciais ameaças relacionadas ao tema de infraestrutura física (Tabela 6). A matriz foi elaborada com base na Metodologia de Gestão de Riscos Corporativos da Embrapa (Embrapa, 2025).

Tabela 6. Matriz de riscos para infraestrutura física.

Processo	Gestão da Infraestrutura Física
Objetivo	Executar a gestão da logística, da frota, manutenção das instalações, de infraestrutura e de segurança da Embrapa.
Ativo	–

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R01	Invasão por pessoas não autorizadas e acesso indevido a áreas restritas	Falhas nos sistemas de controle de acesso; credenciais de acesso roubadas ou perdidas; uso indevido de cartões magnéticos ou senhas.	Prejuízos financeiros; perda de dados confidenciais; danos à reputação da Empresa; riscos à segurança dos empregados.	Registro de visitantes nas guaritas; identificação e cadastro de visitantes nas recepções; monitoramento por vídeo e vigilância.	Baixa	Alto	Médio	Tratar
R02	Roubo de dados de pesquisa ou patentes	Falhas nos sistemas de controle de acesso; credenciais de acesso roubadas ou perdidas; uso indevido de cartões magnéticos ou senhas; segurança inadequada dos laboratórios, acesso indevido a dados de pesquisa, negligência humana.	Prejuízos financeiros; perda de dados confidenciais; danos à reputação da Empresa.	Registro de visitantes nas guaritas; identificação e cadastro de visitantes nas recepções; monitoramento por vídeo e vigilância.	Baixa	Alto	Médio	Tratar
R03	Segurança do perímetro – Invasão da propriedade e vandalismo	Falhas na segurança do perímetro, como cercas danificadas, portões fracos, falta de vigilância; falta de treinamento dos empregados sobre os procedimentos de segurança; negligência por parte dos empregados ou da equipe de segurança.	Roubo de equipamentos e materiais; danos às instalações da Empresa; prejuízos financeiros e perda de produção e produtividade.	Controle realizado pelas guaritas e por ronda motorizada diurna e noturna; perímetro cercado por alambrado e concertina. Uma vez identificado dano durante a ronda, é providenciado reparo.	Baixa	Baixo	Baixo	Tratar
R04	Desastres naturais	Eventos climáticos extremos.	Danos às instalações e interrupção das atividades da Empresa.	Sistema de para raios; manutenção preventiva e constante dos sistemas hidráulico, elétrico e grupo gerador.	Média	Médio	Médio	Tratar
R05	Incêndio	Falhas elétricas, curto-circuito; falhas nos sistemas de proteção contra incêndio, como *sprinklers* ou extintores de incêndio; falta de treinamento dos empregados sobre os procedimentos de segurança; negligência por parte dos empregados ou da equipe de segurança.	Danos materiais à Empresa, incluindo equipamentos, dados e documentos; perda de experimentos e produtividade causando interrupção das atividades da Empresa; prejuízos financeiros; morte ou ferimentos de pessoas, riscos à segurança dos empregados.	Sistema de combate a incêndio formado por dispositivos que visam proteger o patrimônio físico e a vida das pessoas em uma situação de incêndio, tais como rede de hidrantes, extintores, detectores de calor, quadro de comando, portas corta-fogo, alarmes sonoros, *sprinklers* e visuais, entre outros; equipe treinada para agir em caso de emergência; realização periódica de treinamento do público/empregados para ações emergenciais em caso de incêndio.	Alta	Alto	Alto	Tratar

Continua...

Tabela 6. Continuação.

Identificação do risco	Risco	Causa	Consequência	Identificação do controle	Probabilidade	Impacto	Nível do risco	Resposta ao risco
R06	Explosões	Negligência por parte dos empregados; acidentes com produtos químicos ou gases inflamáveis.	Danos materiais à Empresa, incluindo equipamentos, dados e documentos; perda de produtividade e interrupção das atividades da Empresa; prejuízos financeiros; morte ou ferimentos de pessoas, riscos à segurança dos empregados.	Riscos minimizados por equipe treinada; manutenção preventiva e corretiva, e participação da área de segurança do trabalho e da Comissão Interna de Prevenção de Acidentes (Cipa) em treinamentos e ações.	Baixa	Médio	Médio	Tratar
R07	Falhas de energia	Quedas de energia, falhas elétricas, curto-circuito.	Danos materiais à Empresa, incluindo equipamentos, dados e documentos; perda de produtividade e interrupção das atividades da Empresa; prejuízos financeiros.	Grupo gerador – sustenta a carga elétrica de tomadas e iluminação; equipe treinada e qualificada para ações em caso de curto-circuito ou emergências elétricas.	Média	Alto	Alto	Tratar

Prevenção

Todos os empregados e colaboradores da Embrapa devem receber treinamentos periódicos sobre os riscos de segurança e as melhores práticas para conduta e proteção das áreas e ambientes dentro da Empresa.

As áreas de SI e de Gestão de Pessoas da Embrapa devem disponibilizar, para todos os empregados, treinamentos regulares sobre boas práticas de SI, como o uso adequado dos sistemas, a importância das senhas fortes e o reconhecimento de possíveis ameaças. Adicionalmente, devem incentivar uma cultura organizacional que valorize a SI e encoraje os empregados a relatar qualquer incidente ou comportamento suspeito.

Todas as Unidades da Embrapa e a Sede devem utilizar controles de acesso às áreas internas em níveis crescentes em razão da proximidade que a barreira estiver em relação ao ativo de informação, iniciando-se pela portaria externa ou guarita até as instalações críticas, como salas-cofre, *datacenters* e laboratórios.

Todas as UCs e UDs e a Sede devem possuir e utilizar sistema de monitoramento por câmeras que utilize tecnologia e recursos com a capacidade de monitorar e controlar aplicativos, dispositivos e usuários em tempo real. Os sistemas de monitoramento e as tecnologias utilizadas devem receber manutenções periódicas para correções e atualizações.

Também devem utilizar o serviço de vigilância presencial para coibir ameaças por ações humanas, como roubos, depredações, vandalismos e invasões.

As instalações físicas das Unidades e da Sede devem possuir sistema de escoamento de águas pluviais, sistema de para-raios e cercamento para prevenir alagamentos, descargas elétricas e invasões de suas instalações físicas e consequentemente prevenir incidentes de segurança da informação.

Por fim, as UCs e UDs e a Sede devem possuir grupos geradores de energia para os casos de interrupção de fornecimento pela concessionária local, além de utilizar equipamentos de detecção e proteção contra incêndios.

A manipulação de produtos químicos e/ou inflamáveis só podem ser realizada por pessoas preparadas e autorizadas, seguindo todas as normas e procedimentos de segurança relativos à utilização desses produtos.

Detecção

A comunicação inicial de um incidente de segurança envolvendo algum ativo da infraestrutura física pode ser feita por qualquer fonte ou pessoa interna ou externa à

Embrapa. A comunicação por via diferente daquela diretamente ligada ao responsável pelo processo ou ativo afetado, em hipótese alguma, será considerada como motivo para o não conhecimento do incidente.

O monitoramento dos riscos sobre a infraestrutura física deve ser feito pela área responsável pela administração do ambiente físico e instalações na Sede e nas Unidades da Embrapa, por meio de sistema de monitoramento por câmeras, serviço de vigilância presencial e manutenções preventivas das instalações prediais.

Tratamento

Uma vez detectado um incidente de segurança envolvendo algum ativo da infraestrutura física, ele deve ser tratado e analisado para que sejam, na medida do possível, preservadas todas as evidências do incidente, possibilitando-se o rastreamento e identificação de suas causas posteriormente. O tratamento e a análise do incidente devem ser realizados observando-se a definição dos seguintes atributos:

- Unidade e setor onde ocorreu o incidente.
- E-mail, telefone ou outro contato disponível do informante do incidente.
- Data e horário que o incidente foi identificado.
- Descrição e consequência do incidente.
- Ativo de informação afetado pelo incidente.
- Ativo da infraestrutura física afetado.
- Criticidade do incidente.

Resposta

A partir da confirmação de um incidente envolvendo um ativo da infraestrutura física, deve ser feita uma rápida avaliação do risco de propagação da ameaça que o causou, bem como agir para que a ameaça não se propague e executar as seguintes ações:

- Restringir o acesso à área afetada para evitar danos adicionais e facilitar a investigação.
- Desligar os sistemas e dispositivos afetados para minimizar o risco de propagação do incidente.
- Determinar o impacto do incidente nos sistemas, áreas de segurança e operações da Empresa.

- Determinar as medidas de recuperação necessárias para restaurar os sistemas e áreas afetados.
- Restaurar os sistemas e áreas afetados o mais rápido possível, utilizando-se backups ou outras medidas de recuperação e segurança.
- Restabelecer os serviços afetados no menor tempo possível.
- Apurar as responsabilidades de acordo com as leis e normas vigentes.

Pós-incidente

Após a resposta ao incidente, deve ser agendada uma reunião de lições aprendidas entre os envolvidos nos processos afetados pelo incidente, a área responsável pela SI na Embrapa e a área responsável pela administração do ambiente físico e instalações, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos, inclusive deste PSI.

REFERÊNCIAS

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**: seção 1, p. 1, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 11 dez. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 dez. 2024.

BRASIL. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial da União**: seção 1, p. 455, 9 jan. 1991. Disponível em: https://www2.camara.leg.br/legin/fed/lei/1991/lei-8159-8-janeiro-1991-322180-norma-pl.html. Acesso em: 11 dez. 2024.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. **Diário Oficial da União**: seção 1, n. 93, p. 8.353, 15 maio 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 11 dez. 2024.

BRASIL. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. **Diário Oficial da União**: seção 1, p. 3, 20 fev. 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em: 11 dez. 2024.

BRASIL. Resolução nº 44, de 14 de fevereiro de 2020. Dá nova redação aos artigos 1º, 2º e 3º e respectivos anexos 1, 2 e 3 da Resolução nº 40, de 9 de dezembro de 2014. **Diário Oficial da União**: seção 1, n. 36, p. 74-75, 20 fev. 2020. Disponível em: https://dspace.mj.gov.br/bitstream/1/2204/1/RES_CONARQ_2020_44.pdf. Acesso em: 11 dez. 2024.

EMBRAPA. Secretaria Geral. **Manual de Gestão Documental Arquivística**. 2. ed. rev. e ampl. Brasília, DF, 2020. Disponível em: https://www.infoteca.cnptia.embrapa.br/infoteca/bitstream/doc/1129473/1/MANUAL-GESTAO-DOCUMENTAL-ARQUIVISTICA-ed02-2020.pdf. Acesso em: 5 fev. 2025.

EMBRAPA. **Metodologia de Gestão de Riscos Corporativos**. Aprovada na 6ª Reunião Ordinária do Comitê de Riscos, Integridade, Conformidade e Controles Internos da Embrapa – CGRIC. Brasília, DF, 2025. 32 p.

Literatura recomendada

EMBRAPA. **Deliberação de Diretoria nº 19, de 10 de agosto de 2021**. Aprova a versão revisada nº 1 da Norma nº 037.001.002.002, intitulada "Gestão Documental Arquivística e Uso do Sistema Eletrônico de Informações (SEI)", integrante do Manual de Normas da Embrapa. **Boletim de Comunicações Administrativas**, ano XLVII, n° 38 de 16 ago. 2021.

EMBRAPA. **Deliberação de Diretoria nº 29, de 3 de novembro de 2021**. Aprova a Norma nº 037.013.004.002, intitulada "Uso de Dados para Negócios da Embrapa", integrante do Manual de Normas da Embrapa. **Boletim de Comunicações Administrativas**, ano XLVII, nº 51 de 8 nov. 2021.

EMBRAPA. **Deliberação de Diretoria nº 8, de 31 de março de 2020**. Aprova a Norma nº 037.005.001.016, nº 037.005.001.016, intitulada "Acesso e Tratamento da Informação", integrante do Manual de Normas da Embrapa. **Boletim de Comunicações Administrativas**, ano XLVI, n° 23, de 7 maio 2020.

EMBRAPA. **Resolução do Conselho de Administração nº 184, de 4 de abril de 2019**. Aprova a Norma nº 037.005.001.015, intitulada "Política de Governança de Dados, Informação e Conhecimento da Embrapa", integrante do Manual de Normas da Embrapa. **Boletim de Comunicações Administrativas**, ano XLV, nº 16, de 5 abr. 2019.

EMBRAPA. **Resolução do Conselho de Administração nº 225, de 30 de maio de 2022**. Aprova a Norma nº 037.009.002.002, intitulada "Código de Conduta, Ética e Integridade da Embrapa", integrante do Manual de Normas da Embrapa. **Boletim de Comunicações Administrativas**, ano XLVIII, nº 25, de 1 jun. 2022.

EMBRAPA. **Resolução Normativa nº 20, de 3 de junho de 2013**. Estabelece as condições para a determinação do grau de classificação do sigilo das informações, no âmbito da Embrapa. **Boletim de Comunicações Administrativas**, ano 39, n° 22, de 3 jun. 2013.

EMBRAPA. Secretaria de Pesquisa e Desenvolvimento. **Nota Técnica sobre o processo de Gestão de Dados de Pesquisa**, de 18 fev. 2022. Disponível em: https://www.embrapa.br/documents/32009307/68432389/Nota+Técnica+Processo+GDP/eeef0921-cce6-6230-e7ec-53b1e8754154?version=1.1. Acesso em: 5 fev. 2025.

EMBRAPA. Secretaria Geral. **Manual dos indicadores de produção técnico-científica**: orientações para registro no Ainfo. Brasília, DF, 2019. 37 p. Disponível em: https://ainfo.cnptia.embrapa.br/digital/bitstream/item/199537/1/Manual-dos-indicadores-de-producao-Tecnico-Cientifica-Ainfo-ed-01-2019.pdf. Acesso em: 6 fev. 2025.

GLOSSÁRIO

Para efeito deste Plano de Segurança da Informação (PSI), este documento apresenta os seguintes termos, siglas e definições:

Acessibilidade: garantia de que todos os indivíduos, independentemente de suas habilidades ou necessidades, possam acessar e utilizar os recursos de forma segura e eficaz. Isso inclui pessoas com deficiência, mobilidade reduzida, gestantes, idosos e pessoas com necessidades sensoriais.

ANPD: Autoridade Nacional de Proteção de Dados.

Armazenamento: guarda de documentos em local apropriado.

Autenticação: processo que verifica a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo.

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.

Autorização: processo que ocorre após a autenticação e que tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence; portanto, autorização é o direito ou a permissão de acesso a um recurso de um sistema.

Avaliação: processo de análise de documentos arquivísticos que estabelece seus prazos de guarda e sua destinação de acordo com os valores que lhes são atribuídos.

Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

CC BY-NC: Atribuição Não Comercial Creative Commons. Esta licença permite que outros remixem, adaptem e criem a partir do seu trabalho para fins não comerciais. Embora novos trabalhos tenham de lhe atribuir o devido crédito e não possam ser usados para fins comerciais, os usuários não têm de licenciar esses trabalhos derivados sob os mesmos termos.

Completeza: atributo de um documento arquivístico que se refere à presença de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo a que pertence, de maneira a ser capaz de gerar consequências.

Controle ambiental: monitoramento e controle da temperatura, umidade e outros fatores ambientais que podem afetar os equipamentos da empresa.

Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.

CTI: Comitê Técnico Interno das Unidades Descentralizadas e da Sede.

Custódia: responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade.

Dados abertos: dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença que permita sua livre utilização, consumo ou cruzamento, sob a única exigência do crédito à autoria ou à fonte.

Dados de pesquisa, desenvolvimento e informação (PD&I): dados brutos e dados resultantes dos projetos de PD&I, como registros factuais (pontuações numéricas, registros textuais, imagens, sons, entre outros) produzidos e/ou utilizados como fontes primárias para a pesquisa científica e tecnológica, necessários para o desenvolvimento e validação dos seus resultados.

Dados pessoais: dados relacionados à pessoa natural identificada ou 'identificável' — aquela que pode ser reconhecida, direta ou indiretamente, a partir de um identificador, como um nome, número de identificação, dados de localização, identificador on-line ou um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

Dados: sequência de símbolos ou valores, produzidos como resultado de um processo natural ou artificial e representados em qualquer meio.

Documento arquivístico: documento produzido ou recebido no curso de uma atividade prática como instrumento ou resultado dessa atividade, retido para ação ou referência.

Documento arquivístico digital: documento digital reconhecido e tratado como um documento arquivístico.

Edificações: construções em geral que integram os imóveis como estruturas rígidas utilizadas para desenvolver as atividades de uma empresa, que não podem ser separadas do solo e que são projetadas para abrigar e proteger pessoas, operações, produtos e insumos, documentos e bens móveis, incluindo as máquinas e equipamentos que podem conter ativos de informação, contra acessos não autorizados, roubo, perda, corrupção ou destruição. São tipos de edificações os prédios, casas e galpões.

Gestão arquivística de documentos: conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos arquivísticos em fases corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente.

Gestão de dados: processo que contempla as atividades de planejamento, aquisição, organização, estruturação, curadoria e análise de dados, utilizando-se, para isso, ferramenta computacional apropriada para o armazenamento e a recuperação de dados, levando-se em consideração as questões relativas à preservação, à organização, ao compartilhamento, à proteção e à confidencialidade desses dados, bem como o seu acesso e disponibilização para a sociedade quando cabível.

Grupo de acesso: empregados ou colaboradores que exercem cargos, funções ou atividades que lhes garantam acesso a informações, áreas, instalações e materiais de natureza restrita.

Imóveis: áreas de terra que, independente da formalidade, esteja legalmente sob o uso, posse ou propriedade de uma empresa, incluindo o seu subsolo e o espaço aéreo correspondente, além do solo do terreno e tudo quanto se lhe incorporar natural ou artificialmente, em especial as edificações e as instalações, assim como as plantações, cursos e corpos d'água.

Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Indisponibilidade: impossibilidade de acesso aos dados.

Instalações: sistema composto por materiais e equipamentos necessários para assegurar o funcionamento e a segurança das edificações, o qual inclui as instalações hidráulicas e sanitárias, as elétricas e eletrônicas (p.ex. circuitos fechados de TV e cabeamento estruturado), as mecânicas e de utilidades (p.ex. gás, oxigênio e vácuo) e as instalações de prevenção e combate a incêndio.

Incêndio: combustão que pode causar danos à propriedade ou colocar em risco a vida humana.

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

Informações financeiras: dados relacionados à situação financeira de uma empresa.

Informação pessoal: informação relacionada à pessoa natural identificada ou identificável.

Informação restrita: informação protegida por legislação específica. Trata-se de informação cujo acesso será restrito a empregado(a) que possua justificada necessidade de conhecer.

Informação sigilosa: informação submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e aquela abrangida pelas demais hipóteses legais de sigilo.

Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

LGPD: Lei Geral de Proteção de Dados Pessoais.

Malware: software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits.

Metadados: representam "dados sobre dados", fornecendo os recursos necessários para entender os dados no decorrer do tempo, ou seja, são dados estruturados que fornecem uma descrição concisa a respeito dos dados armazenados e que permitem encontrar, gerenciar, compreender ou preservar informações a respeito dos dados ao longo do tempo.

Patentes: título de propriedade intelectual que protege uma invenção ou processo inovador.

PD&I: pesquisa, desenvolvimento e inovação.

Proteção contra incêndio: conjunto de medidas que visam prevenir e combater incêndios.

Repositório digital: um complexo que apoia o gerenciamento dos materiais digitais pelo tempo que for necessário. É formado por elementos de hardware, software e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos.

Restrição de acesso: limitação do acesso às áreas de uma empresa — como salas de servidores, data centers e áreas externas — a pessoas autorizadas.

Segurança cibernética: ações voltadas para a segurança de operações, visando 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.

Segurança contra desastres naturais: conjunto de medidas que visam proteger a empresa contra os impactos de desastres naturais.

Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Segurança do perímetro: conjunto de medidas que visam proteger a área física de uma empresa contra invasões e danos.

Segurança física: proteção física dos ativos de uma empresa contra roubo, vandalismo, danos e desastres naturais.

Sistema de acesso: conjunto de ferramentas que se destina a controlar e a dar a uma pessoa permissão de acesso a um recurso.

Sistema de Detecção de Intrusão (*Intrusion Detection System* – IDS): refere-se a um mecanismo que, sigilosamente, ouve o tráfego na rede para detectar atividades anormais ou suspeitas e, deste modo, reduz os riscos de intrusão. Existem duas famílias distintas de IDS: os N-IDS (*network based intrusion detection system* ou sistema de detecção de intrusões de rede), que garantem a segurança dentro da rede e os H-IDS (*host based intrusion detection system* ou sistema de detecção de intrusões no host), que asseguram a segurança no host.

Sistema de Prevenção de Intrusão (*Intrusion Prevention System* – IPS): monitora o tráfego da rede em busca de possíveis ameaças e as bloqueia automaticamente, alertando a equipe de segurança, terminando conexões perigosas, removendo conteúdo malicioso ou acionando outros dispositivos de segurança.

TIC: tecnologia da informação e comunicação.

Tramitação: curso do documento desde sua produção ou recepção até o cumprimento de sua função administrativa. Também denominado trâmite ou movimentação.

Trilhas de auditoria: conjunto de informações registradas, o qual permite o rastreamento de intervenções ou tentativas de intervenção feitas no documento arquivístico digital ou no sistema computacional.

MINISTÉRIO DA
AGRICULTURA E
PECUÁRIA

GOVERNO FEDERAL

UNIÃO E RECONSTRUÇÃO

CGPE 18905