Informações sobre a Política de Segurança Cibernética

Sumário

1. Introdução

Este documento consiste em uma versão simplificada da Política de Segurança Cibernética que tem como objetivo demonstrar em linhas gerais, os controles adotados para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Os objetivos principais da Política são:

1) Garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, empregados e fornecedores;
2) Proteger adequadamente os sistemas e informações;
3) Garantir a continuidade dos negócios, protegendo os processos críticos de interrupções;
4) Garantir que sejam respeitadas as finalidades aprovadas durante a prestação de serviços de terceiros quando da contratação de serviços de processamento e/ou armazenamento de dados.

Neste contexto, o Grupo Edenred Brasil possui uma gestão de segurança da informação, incluindo políticas, controles e processos de gerenciamento de riscos que asseguram a confiabilidade de seus sistemas e a continuidade dos serviços relevantes para a prestação de serviços. As referidas políticas, controles e processos de segurança estão alinhados às melhores práticas e padrões internacionais de mercado, buscando garantir a conformidade com as leis e regulamentos aplicáveis à segurança da informação, privacidade e proteção de dados.

2. Escopo da política de segurança

A Política de Segurança do Grupo Edenred Brasil, que é revisada periodicamente, promove a implantação de medidas preventivas, detectivas e corretivas voltadas ao controle do ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de vulnerabilidades.

3. Abrangência

As informações divulgadas neste documento deverão ser observadas por todo o Grupo Edenred, incluindo seus acionistas, diretores, gestores, colaboradores e terceiros no exercício de suas atividades, que atuem em nome da empresa ou participem da operação de processos de sua cadeia produtiva.

4. Terminologia

Para a Política Cibernética, os termos abaixo possuem as seguintes definições:

- Segurança da Informação: conjunto de práticas, políticas, conceitos de segurança, abordagens de gestão de risco, treinamentos e tecnologias utilizados para proteger o ambiente cibernético, a organização, a continuidade dos negócios e os dados dos clientes, funcionários, fornecedores ou parceiros de negócios.

- Incidente de Segurança: Um incidente de segurança pode ser definido como qualquer evento que explora alguma brecha/vulnerabilidade, de processos, de soluções, de produtos, sistemas, infraestrutura de TI, entre outros, cujo resultado pode:

  - Causar danos ao negócio e/ou aos colaboradores e/ou clientes, ou;
  - Afetar a habilidade de entregar serviços apropriados aos clientes, ou;
  - Resultar em roubo/ fraude.

- Incidente Cibernético: Também conhecido como incidente de segurança cibernética, incidente de segurança de TI e / ou um incidente de segurança da informação é definido como: Uma ocorrência que compromete a confidencialidade, integridade e/ou a disponibilidade de um sistema e/ou as informações que o sistema processa, armazena ou transmite e que, portanto, constitui uma violação ou ameaça iminente à informação, assim como aos regulamentos internos, políticas, procedimentos e padrões de segurança definidos.

- Vulnerabilidades: quaisquer condições que, quando exploradas por uma pessoa desconhecida ou não vinculada (mas pode ser um funcionário também) mal-intencionado, possam resultar em violações de segurança, tais como falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede, desatualização ou ausência de mecanismos de segurança cibernética. Um ataque de exploração de vulnerabilidades ocorre quando um atacante tenta executar ações maliciosas, como por exemplo invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar uma aplicação ou serviço indisponível.

5. Monitoramento de segurança da informação

O processo de monitoramento de segurança da informação e prevenção contra ciberataques consiste em identificar ameaças e vulnerabilidades, definir controles de segurança necessários à proteção do negócio, testar e monitorar ambientes internos e externos. O objetivo principal é evitar a concretização de ameaças cibernéticas.

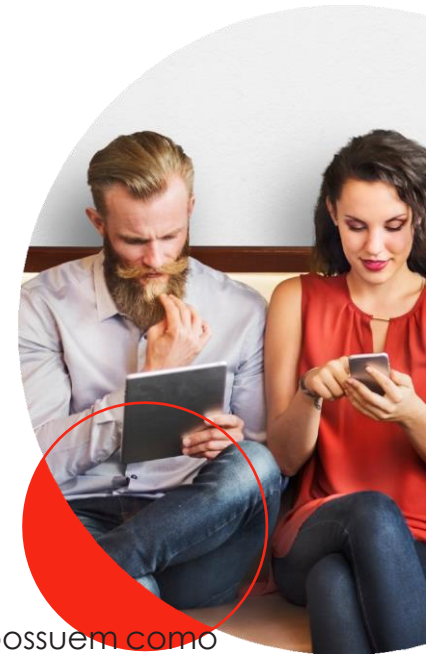
6. Gestão de segurança das aplicações

As principais premissas aplicáveis à adoção de novas tecnologias englobam:

- O desenvolvimento de novas aplicações deve estar alinhado às melhores práticas de segurança e diretrizes, relacionadas com o desenvolvimento seguro;
- A implantação de controles e mecanismos de rastreabilidade das informações; A realização de testes de segurança, como teste de penetração, avaliação de vulnerabilidades e teste de código seguro, também deve ser executada para os serviços relevantes antes da implementação no ambiente de produção;
- A realização de testes de segurança gerais, como, por exemplo, adequação aos parâmetros de segurança); e,
- Controles que assegurem a segregação entre os ambientes de desenvolvimento, teste e produção, com o objetivo de reduzir os riscos de acessos não autorizados ou alterações indevidas no ambiente operacional, banco de dados e/ou aplicações.

7. Gestão de controle de acessos

- Estabelecer o acesso restrito às pessoas que tenham necessidade de utilizá-las para suas atividades no Grupo Edenred Brasil por todo ciclo de vida da informação.
- Gerenciamento de acesso e identidade aos sistemas, certificando a autenticidade e rastreabilidade dos acessos;



8. Continuidade de negócios

Os controles adotados no desenvolvimento de infraestrutura possuem como objetivo primário garantir que se mantenha operacional frente a ameaças cibernéticas, de modo a assegurar a confidencialidade, a integridade e a disponibilidade da informação, de modo a garantir a continuidade dos negócios por meio de análise de cenários, monitoração e testes para a melhoria contínua.

9. Plano de respostas de incidentes de segurança cibernética

O plano de respostas a incidentes deve conter etapas de classificação, investigação da causa raiz, aplicação de ações corretivas (quando aplicável, ações preventivas) e comunicação as partes interessadas, assegurando que cada incidente seja tratado de acordo com seu impacto e urgência.

10. Gestão de empresas prestadoras de serviços relevantes

A Edenred Brasil adota procedimentos para contratação de fornecedores de serviços de processamento e armazenamento de dados e de computação em nuvem compatíveis com o disposto na Resolução nº. 4.893/2021 do Banco Central do Brasil.

Na gestão de seus fornecedores, o grupo Edenred Brasil busca, principalmente, garantir a execução de controles para prevenção de incidentes a serem adotados por fornecedores que manuseiam dados sensíveis ou que sejam relevantes para as atividades. Além disso, os referidos controles devem ser compatíveis com os processos e mecanismos de segurança cibernética adotados.

11. Contato

Em caso de dúvidas, acione a marca da Edenred com a qual você possui negócios. Contatos disponíveis em https://edenred.com.br/contato/.

12. Aviso legal

Este documento foi elaborado para fins informativos. Este documento não pode ser reproduzido (no todo ou em parte) por qualquer pessoa, para quaisquer finalidades, sem a prévia expressa autorização do grupo Edenred Brasil. Eventuais violações estarão sujeitas às penas da lei.

13. Referências

- Norma ABNT NBR ISO 27001:2022 – Sistemas de Gestão da Segurança da informação.
- Resolução nº 85/2021 – Segurança cibernética e contratação de serviços em nuvem - Banco Central do Brasil.
- Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).


Edenred