Cartilha

A segurança da informação na

Edenred Brasil

Sumário

1. A Segurança da Informação na Edenred Brasil

A Edenred Brasil e suas empresas **(Ticket, Ticket Log, Edenred Soluções Pré-Pagas, Repom e Freto)** apresentam as diretrizes relacionadas à Segurança da Informação.

Nosso documento principal é a **Política Corporativa de Segurança da Informação**, que tem como objetivo estabelecer os princípios, práticas e diretrizes; manter e desenvolver a cultura organizacional baseada nos conceitos de Segurança da Informação e do ambiente cibernético, além de promover a melhoria contínua das medidas de controle que irão resultar na mitigação de riscos.

As diretrizes definidas neste documento devem ser observadas por todas empresas da Edenred no Brasil, incluindo acionistas, diretores, gestores, colaboradores, prestadores de serviço e fornecedores no exercício de suas atividades, que atuem em nome da empresa ou participem da operação de processos de sua cadeia produtiva.

2. Quem é quem?

A Edenred Brasil possui uma estrutura que visa identificar, avaliar e tratar os riscos associados ao negócio, processos, projetos e consequentemente aos riscos relacionados à Segurança da Informação. Para isso, a Coordenação de Segurança da Informação (CSI) é responsável por definir as diretrizes por meios de Políticas, Normativos e Procedimentos.

Além disso, esta coordenação cuida da gestão de acessos, da prevenção contra vazamento da informação, do monitoramento da marca, do apoio à TI e ao Negócio quanto a implementação de boas práticas e da conscientização dos usuários, prestadores de serviço e stakeholders em geral.

A CSI é subordinada à Gerência Corporativa de Riscos, gerência a cargo de outras áreas como Prevenção à Fraude, Risco Operacional & Continuidade e Riscos Financeiros.

Ainda, na TI do Grupo, há a área de IT Security, responsável pela gestão de Firewalls, scan de vulnerabilidades, antivírus, spam, entre outras importantes atividades.

3. Princípios de Segurança da Informação

A Edenred Brasil se baseia no conjunto de práticas amplamente estabelecido pelo mercado e no que acredita como importantes fatores a serem observados para garantir uma boa maturidade quanto à Segurança da Informação. Abaixo nossos pilares:

Confidencialidade: garantir que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;

Disponibilidade: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;

Integridade: garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

4. Diretrizes de Segurança da Informação que respeitamos

A Edenred Brasil estabelece as melhores práticas quando o assunto é Segurança da Informação, nossas principais diretrizes você pode observar a seguir:

a) **Sigilo da informação e ética:** as informações da Edenred Brasil, dos seus clientes e do público em geral a que o Grupo obtém acesso para desempenhar suas atividades devem ser tratadas de forma ética e com o grau de sigilo necessário e de acordo com as leis vigentes, aderente ao regulador do segmento de negócios e as normas internas, evitando-se mau uso e exposição indevida;

b) **Transparência e finalidade:** a informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;

c) **Coibir o conflito de interesse:** todo processo, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador ou equipe de colaboradores;

d) **Autorização:** o acesso às informações e recursos só deve ser feito se devidamente autorizado;

4. Diretrizes de Segurança da Informação que respeitamos

e) **Identificação única:** a identificação de qualquer Colaborador e prestador de serviços deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas. A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;

f) **Menor acesso possível:** a concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;

g) **Comunicação centralizada:** os riscos às informações devem ser reportados à área de Segurança da Informação assim como o deve haver registro relacionados a incidentes de Segurança da Informação;

h) **Divulgação:** as responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, prestadores de serviço e fornecedores que por sua vez devem entender e assegurar estas diretrizes;

i) **Proteção da Informação:** a informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação em todo o seu ciclo de vida como: Geração, Manuseio, Armazenamento, Transporte e Descarte;

j) **Conformidade:** estar em conformidade com a legislação vigente é a base para nossa segurança.

5. Controles de Segurança que exigimos

Em termos práticos e em conformidade com as normas do Banco Central, todos os nossos **parceiros e fornecedores** devem garantir minimamente:

a) A rastreabilidade, integridade e a segurança das informações e dos acessos;

b) A proteção da informação e seu manuseio, seja por meio de criptografia no armazenamento e na transmissão por protocolos atualizados e reconhecidos pelo mercado;

c) A adoção de padrão de proteção conforme relevância e sensibilidade das informações;

d) A segurança dos sistemas e aplicações baseando-se em frameworks como OWASP, por exemplo;

e) A prevenção contra vazamento ou utilização indevida de dados afim de não comprometer as marcas e gerar concorrência desleal e descumprimento à legislação;

f) O tratamento dos incidentes de Segurança da Informação, incluindo formalização, causa, efeitos e reporte;

5. Controles de Segurança que exigimos

g) O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

h) A identificação e a segregação dos dados dos usuários finais da instituição por meio de controles físicos ou lógicos;

i) Manter a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da instituição.

6. Nosso norte

Abaixo, algumas das referências pelas quais nos baseamos e que são nosso norte para as boas práticas da Segurança da Informação:

I. Circular n. 3.681, de 4 de novembro de 2013 – Banco Central do Brasil.

II. Norma ABNT NBR ISO/IEC 27001:2013 – Sistemas de gestão da segurança da informação.

III. Resolução nº 4.658, de 26 de abril de 2018 – Segurança cibernética e contratação de serviços em nuvem - Banco Central do Brasil.

IV. CIRCULAR Nº 3.909, DE 16 DE AGOSTO DE 2018 - Segurança cibernética e contratação de serviços em nuvem - Banco Central do Brasil.

IV. Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

A proteção da informação, sua integridade, confidencialidade e disponibilidade é responsabilidade de todos! Junta-se às nossas práticas e ajude-nos a cada vez mais termos uma relação confiável.

Segurança da Informação
Gerência Corporativa de Riscos


Edenred