1 Objetivo

Estabelecer as diretrizes quanto à política de segurança da informação e segurança cibernética, garantindo a integridade, confidencialidade, legalidade, autenticidade e proteção dos dados utilizados na realização dos negócios da EMPRESTA Capital.

A Política de Segurança da Informação e Segurança Cibernética objetiva proteger a informação de diversos tipos de ameaças, visando garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio, bem como:

- Definir diretrizes para a segurança do espaço cibernético relacionadas à capacidade da EMPRESTA Capital de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
- Proteger as informações sob responsabilidade das entidades preservando sua confidencialidade, integridade, disponibilidade e autenticidade;
- Prevenir eventuais interrupções, totais ou parciais, dos serviços de TI acessados pela EMPRESTA Capital e, no caso de sua ocorrência, reduzir os impactos dela resultantes;
- Tratar e prevenir incidentes de segurança cibernética;
- Formar e qualificar os recursos humanos necessários à área de segurança cibernética;

2 Referências

Resolução 4.893/2021 – Banco Central - Risco Cibernético;

NBR ISO/IEC 17799:2005;

ABNT 21:204.01-010;

Lei 9.609/98 – Lei do Software;

Lei 13.709/2018 – LGPD.

3 Procedimentos e Controle

- Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, a EMPRESTA Capital adota procedimentos e controles, conforme porte e perfil de risco da entidade. Estes procedimentos e controles são aplicados para sistemas de informação desenvolvidos internamente ou adquiridos junto a terceiros;
- É estabelecido um plano de ação e de resposta a incidentes, revisado anualmente;
- Os incidentes, e respectivas análises do ocorrido e soluções, são reportados pela área de TI/Facilities à Diretoria Executiva em mensagem interna, sempre que ocorrem;
- As informações de propriedade ou sob custódia da EMPRESTA Capital, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados;
- São adotados mecanismos para disseminação da cultura de segurança cibernética na instituição;

- Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a segurança cibernética no âmbito da EMPRESTA Capital, inclusive o Plano de continuidade de Negócios.

4 Princípios

A proteção e privacidade de dados dos clientes refletem os valores da Empresta Capital e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

- São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- Somente serão acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

5 Detalhamento

Diretrizes

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização. Consequentemente, necessita ser adequadamente protegida.

A segurança da informação é aqui caracterizada pela preservação da:

a) **Confidencialidade**, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

b) **Integridade**, que é a salvaguarda da exatidão e fidedignidade da informação e dos métodos de processamento;

c) **Disponibilidade**, garante que a informação possa ser obtida sempre que for necessário, isto é, que esteja sempre disponível para quem precisar dela no exercício de suas funções.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

Atribuições e Programa de Treinamento / Capacitação

Cabe a todos os colaboradores da EMPRESTA Capital, aos Correspondentes Bancários e aos prestadores de serviços de TI:

- Cumprir fielmente a Política de Segurança da Informação;
- Buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados;

- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela EMPRESTA Capital;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela EMPRESTA Capital;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Atender às leis que regulamentam as atividades da Empresta Capital e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- Comunicar imediatamente à área de Segurança Cibernética, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

A Política de Segurança da Informação e Cibernética deve ser divulgada a todos os funcionários e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento, ficando registrado através do Anexo 2 que todos os colaboradores da EMPRESTA Capital tiveram o treinamento adequado por pessoa devidamente instruída sobre todas as informações necessárias em relação aos Riscos de Segurança da Informação e Cibernética.

A EMPRESTA Capital dispõe de Programa de Treinamento e Capacitação para todos os colaboradores, a respeito dos principais tópicos dos Riscos de Segurança da Informação e Cibernética, e Plano de Continuidade do Negócio.

Riscos Cibernéticos

Riscos de ataques cibernéticos são aqueles oriundos de malware, técnicas de engenharia social, invasões, ataques de rede, fraudes externas, que deixam desprotegidos dados, redes e sistemas da instituição causando danos financeiros e de reputação consideráveis.

O risco de ataque cibernético ameaça os princípios da segurança das informações, tais como confidencialidade, integridade e disponibilidade.

O risco da imagem, o risco de continuidade do negócio e os prejuízos financeiros são exemplos de consequências/danos que podem ser causados por falhas na segurança cibernética.

No que se refere especificamente à Malwares, são identificadas as seguintes ameaças:

- Vírus: software que causa danos a máquina, rede, softwares e banco de dados, além da obtenção de informações sigilosas e vendas de dados;
- Trojan: aparece dentro de outro software e cria uma porta para a invasão do computador;
- Spyware: software malicioso para coletar e monitorar o uso de informações;
- Ransomware: software malicioso que sequestra o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

A segurança cibernética deve garantir, minimamente:

i. a segurança dos sistemas e dos bancos de dados;
ii. o gerenciamento das pessoas autorizadas;
iii. a segurança dos sistemas e informações que estão na nuvem;
iv. a segurança para todos os dispositivos/equipamentos;
v. o planejamento da continuidade do negócio; e

vi. o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade da organização.

Com base nas informações acima, a EMPRESTA Capital avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e restabelecimento da segurança devida.

Lei Geral de Proteção de Dados - LGPD

A Lei Geral de Proteção de Dados (LGPD) estabelece regras sobre como os dados pessoais (de pessoa física) devem ser tratados tanto nos meios físicos quanto nos digitais.

Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração é considerada como tratamento de dados pessoais.

Em obediência à Lei Geral de Proteção de Dados (LGPD), e com o intuito de mitigar o risco cibernético de incidentes com dados pessoais, como por exemplo vazamento de dados, a EMPRESTA Capital deverá implementar um Plano de Contingência para tratar incidentes de segurança com dados pessoais. Este terá o objetivo de preparar a Instituição para lidar com a gestão de um incidente de segurança, garantindo que responda de forma mais rápida, organizada e eficiente ao evento, minimizando as consequências para todos os envolvidos.

Engenharia Social

Engenharia social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas.

A Engenharia Social manifesta-se de diversas formas, e podemos dividi-los em dois grupos.

Diretos: São aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido.

Indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir, como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a fazer é ignorar a oferta tentadora e apagar o e-mail imediatamente.

- Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
- Phishing: links transmitidos por e-mails, pesquisas em sites ou ferramentas de buscas (Google, Yahoo, Bing) simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

- Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes Externas: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de muitos computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

Classificação da Informação

É de responsabilidade do Coordenador de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (e-mails, relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

Pública:

É uma informação da EMPRESTA Capital com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija sua publicidade.

Interna:

É uma informação da EMPRESTA Capital que a empresa não tem interesse em divulgar externamente, portanto o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da EMPRESTA Capital.

Confidencial:

É uma informação crítica para os negócios da EMPRESTA Capital ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à EMPRESTA Capital ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

São exemplos de informações confidenciais:

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.)
- Situação financeira e movimentação bancária de clientes;
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

Restrita:

É toda informação que pode ser acessada somente por funcionários da EMPRESTA Capital explicitamente indicados pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Gestão de acessos às informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

Segurança Física e Lógica

O gerenciamento do banco de dados é responsabilidade da Área de TI, assim como a manutenção, alteração e atualização de equipamentos e programas.

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores e terceiros da EMPRESTA Capital são treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa efetivo de conscientização.

Backup (Cópia de Segurança dos Dados)

Todos os dados da EMPRESTA Capital deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias das pastas de rede, arquivos e bancos de dados são de responsabilidade da área de TI, as quais serão feitas diariamente e armazenadas automaticamente em nuvem, ou seja, a Instituição não possui Backup em máquinas locais. O Backup detecta a última alteração e processa os arquivos novos e os alterados, e tem retenção máxima de 3 (três) anos.

Além de Backup, a EMPRESTA Capital dispõe de uma ferramenta complementar utilizada para recuperar suas informações. A Shadow Copy permite criar cópias de segurança de arquivos locais de curto período, e permite ainda a qualquer usuário restaurar e recuperar arquivos sem a necessidade de acionar o programa de backup. Ou seja, a ferramenta salva uma cópia a cada 2 (duas) horas e tem uma retenção de dados de 3 (três) dias.

A ferramenta não substitui o Backup, apenas facilita o trabalho conjunto entre a informação, o backup, o hardware e o software de armazenamento.

O Backup relacionado aos sistemas RBM, é realizado pela própria empresa prestadora de serviços, obedecendo o disposto em contrato cláusula 2.1, Y, e 2.2.1. Cabendo a área de T.I da RPW S/A, solicitar periodicamente ao provedor de sistemas (RBM) as devidas evidências da realização do backup, arquivando em pasta da rede, os pedidos de evidências, as devolutivas do provedor de serviço e relatório de análise do material recebido aprovado pela Diretoria Administrativa Financeira.

Direitos de Propriedade:

Todo produto resultante do trabalho dos Correspondentes (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade da EMPRESTA Capital.

Em caso de extinção ou rescisão do contrato de prestação de serviços de correspondente no país, por qualquer motivo, deverá o Correspondente devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços a EMPRESTA Capital.

Diretrizes quanto ao uso da Internet e E-mail Corporativo:

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

O acesso às páginas e websites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdo impróprio ou mídias sociais.

É vedado qualquer tipo de download, como também o upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização da Diretoria. Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

É proibido o uso do e-mail corporativo para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.

Não deve se executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI. Na dúvida, não clique para abrir o anexo ou link.

Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais (hoax).

Quando estiver fora do ambiente da empresa, não utilizar o e-mail corporativo em redes Wi-Fi públicas (aquelas disponibilizadas em hotéis e aeroportos, por exemplo), especialmente quando lidar com assuntos confidenciais ou restritos. Estas redes Wi-Fi são mais vulneráveis a invasões e ataques de hackers. Nesse tipo de ataque, chamado de *man in the middle*, um dispositivo é configurado para se disfarçar de equipamento de rede, processando todo o tráfego e tentando acessar pacotes com registro de informações sensíveis.

Não enviar dados corporativos para o e-mail pessoal. O envio de e-mails com arquivos anexados pesados será objeto de monitoramento pela Diretoria. O e-mail corporativo não deve ser usado como e-mail pessoal.

Utilização e Conexão de Equipamentos

Somente é permitido o uso de equipamentos homologados e devidamente contratados pela EMPRESTA Capital.

A utilização de equipamentos pessoais por terceiros nas instalações da EMPRESTA Capital e a conexão destes na rede interna e à Internet requer autorização prévia e expressa da Área de Gestão de Riscos e de Compliance, ou da Diretoria Executiva.

Os colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet mediante a autorização prévia da Área de Gestão de Riscos e de Compliance.

A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia e expressa da Área de Gestão de Riscos e de Compliance e da Diretoria Executiva.

A fim de evitar desgastes dos equipamentos, diminuindo seu tempo útil de vida, diariamente, os computadores devem ser desligados de forma automática. Cada setor terá um horário definido para o desligamento, a partir de definição pelo Gestor da área.

Serão passíveis de advertências e de respectiva reparação ou ressarcimento, ações do tipo:

- Mau uso dos equipamentos;
- Remover ou substituir peças, acessórios e periféricos, sem permissão da área de informática;
- Quebra/avaria intencional desses equipamentos.

Para fins de padronização, os papéis de parede e os bloqueios de tela deverão obedecer ao modelo de imagem disponibilizado pela área de Marketing da EMPRESTA Capital, e trocados pela área de TI por novos modelos sempre que houver necessidade de mudança da arte. As imagens de papel de parede e bloqueio de tela não poderão ser trocadas pelos próprios colaboradores.

Controle de Acesso Lógico (Baseado em Senhas)

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

Política de Mesa Limpa (Clean Desk)

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não. Os documentos, particularmente aqueles contendo informações de clientes, devem ser guardados em gavetas ou armários, nunca deixando a vista sob as mesas, principalmente após o expediente.

Não deverão ser reutilizados papéis ou materiais em geral que contenham informações internas ou confidenciais.

Continuidade de Negócios

O processo de gestão de continuidade de negócios, relativo a segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

Incluem-se nesse processo a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

Processamento, Armazenamento de dados e Computação em Nuvem

Conforme a Resolução 4.893/2021 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a EMPRESTA Capital deverá assegurar um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

A EMPRESTA Capital possui dois servidores AD (*active directory*), um local e um em nuvem. Para evitar atrasos de sincronia e perda de dados, bem como para melhorar sua performance, estes servidores são sincronizados no tempo médio de 6 (seis) horas.

Contratação de Terceiros

Caso haja a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, a contratada deve:

- Cumprir a legislação e da regulamentação em vigor;
- Permitir o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- Assegurar a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- Assegurar a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;
- Permitir o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- Assegurar o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- Assegurar a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos;
- Assegurar a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Violação da Política, Normas e Procedimentos de Segurança da Informação

As violações de segurança devem ser informadas à área de TI e a Diretoria. Toda violação ou desvio será investigado para a determinação das medidas necessárias, visando a correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas;
- Mau uso e/ou avaria e quebra intencional dos maquinários.

A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os colaboradores e os Correspondentes às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente para o endereço de e-mail denuncia@emprestacapital.com.br