POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1 - Escopo e Público-Alvo

O escopo compreende a atualização da Política de Segurança da Informação (PSI), estabelecimento de Planos e Normas complementares ao PSI, ampla divulgação e treinamento dos usuários, bem como a efetiva implementação do Sistema de Gerenciamento da Segurança da Informação na empresa.

Todos os usuários com acesso às informações da empresa, independentemente da sua condição (funcionário, estagiário, temporário ou terceiro), que de alguma forma acessem, criem, manipulem ou descartem as informações de propriedade da empresa, em qualquer momento ou forma, digital ou não, devem estar em conformidade com a Política de Segurança da Informação.

A Política de Segurança da Informação aplica-se a todos os ativos de informação, recursos humanos (pessoas), administrativos (processos) e tecnológicos de propriedade e/ou administrados pela empresa. Aplica-se a todos os sistemas operacionais, computadores (desktops, notebooks, tablets) e todos os sistemas de aplicação, sejam de desenvolvimento interno ou externo.

1.1 - Princípios da Política de Segurança

Segurança da Informação são esforços contínuos para proteção dos ativos de informação e deve seguir três paradigmas básicos, considerados os pilares da Segurança da Informação:

Integridade: garantir que as informações ou os recursos da informação estão protegidos contra modificações não autorizadas, mantendo-se íntegros, sem modificações indevidas, acidentais ou propositais;

Confidencialidade: garantir que certas informações sejam de conhecimento exclusivo das pessoas autorizadas, não podendo ser disponibilizadas ou divulgadas sem autorização prévia do proprietário;

Disponibilidade: garantir que as informações estejam acessíveis a todas as pessoas autorizadas que necessitam delas para o desempenho de suas atividades.

2 – Glossário

Acordo de Confidencialidade – cláusula ou instrumento contratual que contém responsabilidades e direitos e deveres dos contratados, tais como leis de direito autorais ou de proteção de dados, bem como a extensão da responsabilidade para fora das dependências da organização e após a rescisão do vínculo contratual.

Ambiente de Desenvolvimento - Instalações de processamento de dados cuja plataforma tecnológica destina-se ao uso exclusivo dos técnicos desenvolvedores de sistemas de informação e aplicativos.

Ambiente de Produção – Instalações de processamento de dados cuja plataforma tecnológica destina-se ao armazenamento e execução dos sistemas de informação e aplicativos, sendo as áreas meio e fim da empresa, como administração, financeiro, recursos humanos, comercial, central de serviços, etc.

Aplicativo – Arquivo executável, autônomo, facilitando a mobilidade e reduzindo o tempo de execução e a realização de tarefa específica pelo usuário.

Ativo – Patrimônio composto por bens e direitos da empresa, composto por hardware, software, pessoas e informação. A informação é um ativo essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida.

Componente de Rede – Equipamento empregado na rede, incluindo sua infraestrutura, para comunicação, gerência e supervisão, incluindo hardware e software.

Configuração – Conjunto de características físicas e funcionais de hardware e software necessárias ao seu adequado funcionamento.

Contingência – Refere à possibilidade de algo acontecer, como a queda do link, e nesta eventualidade possuir condição, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos. Um Plano de Contingência inclui uma série de subplanos, como o plano de backup da qual são introduzidas algumas medidas preventivas para evitar a perda da informação, ou o plano de emergência que especifica qual deve ser a ação no momento de uma ameaça.

Continuidade de Negócios – Conjunto de estratégias e planos que visam garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual faz parte. O Plano de Continuidade de Negócios é um padrão mundial e abrangente, definido pela ISO 27301. A responsabilidade da implementação do Plano de Continuidade de Negócios é dos Dirigentes da organização. A equipe de Responsável pela Segurança da Informação pode auxiliar nessa tarefa, na criação, manutenção, divulgação e coordenação de planos e procedimentos complementares e necessários para uma recuperação efetiva, minimizando os impactos a organização.

Gestores – Gerentes, coordenadores e responsáveis por áreas específicas da empresa.

Proprietário da Informação – Gestor responsável pela concessão, manutenção e revisão das autorizações de acesso à um conjunto de informações.

Responsável pela Política de Segurança – Pessoa designada como Diretor da Tecnologia da Informação, zelando pelo seu cumprimento, guarda e publicidade.

Senha – Serve para autenticar uma conta ou permitir acesso a uma área restrita ou específica, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. Se outra pessoa tiver acesso à senha de alguém, ela poderá usá-las e realizar ações em seu nome, sendo o proprietário da senha responsabilizado.

Sistemas de Informação – Processos responsáveis por coletar e transmitir dados que sejam úteis ao desenvolvimento de produtos ou serviços das empresas, organizações e de demais projetos.

Usuário – Pessoa autorizada a utilizar os serviços prestados pela empresa, como funcionários, estagiários, temporário, terceiro e demais usuários.

Múltiplo Fator de Autenticação (MFA) – Para acesso remoto a rede interna da empresa, será utilizado múltiplo fator de autenticação com intuito de atuar como uma camada adicional de segurança para prevenir que usuários não autorizados acessem a rede.

3 - Diretrizes de Segurança da Informação

As diretrizes a seguir constituem os pilares para o Sistema de Gerenciamento da Segurança da Informação e devem orientar o desenvolvimento das Normas e Procedimentos.

3.1 - Aspectos Gerais

Todas as informações desta Política devem estar disponíveis para qualquer funcionário, estagiário ou terceiro vinculado à informação da empresa.

Ativo é tudo aquilo que tem valor e precisa ser protegido. As informações são ativos, que, assim como outros ativos importantes para os negócios, possuem valor e devem ser protegidos adequadamente.

Os sistemas, as informações criadas e manipuladas, e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da empresa, não podendo ser interpretados como de uso pessoal.

Todos os funcionários, estagiários e prestadores de serviço da empresa devem ter ciência de que o uso dos sistemas, informações e recursos tecnológicos pode ser monitorado e auditado, e que os registros podem servir para detecção de violações desta Política e das Normas de Segurança da Informação. E, conforme o caso, podem servir como evidências em processos administrativos e/ou legais.

Todos devem ter ciência de que o ambiente da empresa pode ser monitorado e auditado através de dispositivos de segurança patrimoniais, como circuitos de vídeo e alarmes. Tais registros e imagens podem ser utilizados nos termos do item anterior e são protegidos nos termos da legislação vigente.

Para garantir o uso adequado e a proteção das informações, as regras relacionadas à Segurança da Informação devem ser atualizadas e disponíveis por meio de Normas específicas.

3.2 - Propriedade da Companhia

As Diretrizes de Segurança da Informação aplicam-se a todos os ativos de informação de propriedade ou administrados pela empresa. Exemplos de ativos incluem sistemas de informação, servidores, equipamentos de informática e relatórios impressos. O uso destes recursos implica no reconhecimento de que todas as informações geradas, de propriedade ou administradas pela empresa, podem ser monitoradas sem aviso prévio ou aprovação dos usuários.

3.3 - Classificação da Informação

Toda informação gerada e/ou utilizada pela empresa deve ser rotulada de acordo com o Plano de Classificação da Informação. Para proteção adequada, toda aplicação, sistema ou informação crítica deve ter um responsável (proprietário) e passar por um critério de classificação baseado na confidencialidade e criticidade para o negócio da empresa, de acordo com o Plano de Classificação da Informação. Uma vez classificada, a mesma deve ser protegida e receber o tratamento adequado.

3.4 - Acesso às Informações

O acesso à informação de propriedade da empresa ou sob sua guarda baseia-se no conceito de que o usuário deve ter um nível de permissão suficiente para executar suas tarefas e não mais do que isso. Para o acesso a sistemas de informação e ambiente de redes, deve-se consultar a

Política de Senhas da empresa, elaborada em conformidade com as definições do proprietário do processo ou da informação em questão.

Serão aplicados controles considerados necessários para garantir que apenas as informações pertinentes às funções exercidas por cada usuário estejam acessíveis quando e onde forem necessárias. Os mecanismos aplicados para garantir o controle de acesso estarão ligados a códigos de acesso únicos, exclusivos e intransferíveis. É responsabilidade do usuário mantê-los em sigilo e, caso necessário, comunicar a perda ou esquecimento destes ao departamento responsável pela gestão de senhas.

Além disso, são necessários:

- Procedimento formal de concessão de acesso aos sistemas, por meio de senhas ou equivalente;
- Remoção imediata de autorizações dadas a usuários afastados ou desligados da empresa ou que tenham mudado de função;
- Remoção periódica das autorizações concedidas, como em caso de afastamento, licença ou férias;
- Regras de atribuição, manutenção e uso de senhas.
- Múltiplo fator de autenticação (MFA), uma camada adicional de segurança para acesso à rede interna.

3.5 - Comportamento Seguro

Independentemente do meio ou forma que a informação se apresenta, todos devem adotar um comportamento seguro para proteção e salvaguarda das informações. Destacam-se os seguintes itens:

- Todos devem assumir uma atitude proativa em relação à proteção da informação;
- Selecionar senhas de qualidade, difíceis de adivinhar;
- Senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros, anotadas em papel ou em sistemas visíveis ou de acesso não protegido;
- Proteger o acesso aos equipamentos através de bloqueio sempre que se ausentar;
- Evitar discutir assuntos confidenciais em áreas com risco de exposição da mesma, tanto no “mundo digital” quanto no “mundo real”;
- Armazenar documentos em locais apropriados de acordo com a classificação, confidencialidade e criticidade.

3.6 - Identificação de Usuário

A empresa define como obrigatório que todos os usuários com acesso aos sistemas de informação possuam uma identificação pessoal, inequívoca e intransferível.

3.7 - Termo de Confidencialidade e Responsabilidade

Antes de receber qualquer tipo de permissão de acesso ao sistema, o usuário deve assinar um termo de confidencialidade e responsabilidade. Uma assinatura nesse termo significa que o usuário tem ciência e concorda em cumprir os regulamentos, normas e procedimentos relacionados à segurança da informação.

3.8 - Critérios de segurança na gestão de terceiros

Os contratos da empresa em questão e empresas prestadoras de serviço que tiverem acesso a informações, aos sistemas ou ambiente tecnológico, devem conter cláusulas de confidencialidade e responsabilidades entre as partes e ainda assegurarem que os profissionais:

- Cumpram a Política e Normas de Segurança da Informação da empresa;
- Cumpram as leis e normas que regulamentam a propriedade intelectual;
- Protejam as informações da empresa;
- Utilizem as informações, sistemas e ambiente tecnológico da empresa apenas para finalidades previamente aprovadas;
- Comuniquem imediatamente qualquer violação desta Política e/ou suas Normas.

3.9 - Segurança Física e do Ambiente

O acesso a locais com informações sensíveis deve ser restrito fisicamente. Toda pessoa com acesso a este tipo de local deve estar com crachá de identificação da empresa. Nas demais dependências físicas da empresa, e somente nela, as pessoas definidas como clientes ou usuários poderão estar utilizando seus crachás ou não, dependendo do critério adotado pelo Gestor da área em questão, na condição de responsável direto pelas informações contidas naquele espaço.

3.10 - Armazenamento de Informações

Os usuários de computadores são responsáveis pelas informações neles armazenadas. Todas as informações consideradas pelo usuário relevantes às suas atividades devem ser armazenadas

nos servidores de arquivos da empresa, respeitando os limites de espaço determinados. Arquivos que não dizem respeito às atividades de trabalho da empresa não devem ser armazenados nos servidores de arquivos.

3.11 - Monitoração e Controle

Para assegurar o efetivo cumprimento da Política de Segurança da Informação, a empresa se reserva o direito de monitorar, inspecionar ou auditar a informação armazenada nos computadores, servidores e sistemas de informação de sua propriedade ou que trafegue pela rede da empresa.

Os usuários devem estar cientes deste direito e não utilizar os sistemas para fins particulares. Todos os recursos de propriedade e/ou administrados pela empresa, armazenados em cópias de segurança, também estão sujeitos à monitoração.

3.12 - Conduta Imprópria

O não cumprimento por parte do usuário de uma diretriz ou norma definida na Política de Segurança da Informação implica em providências estabelecidas nos processos do Recursos Humanos. Havendo necessidade de investigações, os acessos do usuário podem ser revogados temporariamente.

3.13 - Reporte de Incidentes

Incidentes ou eventos que possam ter impacto na segurança das informações devem ser reportados ao Responsável pela Segurança da Informação, através da Central de Serviços da Diretoria de Tecnologia da Informação. Todos os usuários devem estar cientes dos procedimentos para reporte.

3.14 - Legislação

A empresa tem como princípio cumprir as leis e normas aplicáveis aos locais onde está estabelecida. A Política de Segurança da Informação deve estar de acordo com a legislação vigente, sendo solidária a toda situação específica que exista legislação vigente, mesmo não estando expressa na Política.

3.15 - Exceções

As Diretrizes de Segurança da Informação estabelecem as normas e orientações que devem ser seguidas por todos os usuários. A Política de Segurança da Informação deve ser considerada como um instrumento obrigatório. As exceções às normas estabelecidas neste regulamento devem ser formalmente documentadas e aprovadas pelo gestor responsável pela necessidade e um ciente/de acordo do Responsável pela Segurança da Informação, e posteriormente repassadas ao Comitê Gestor para análise e deliberações. Ações em caso de não conformidade, quando não previstas em Normas especificadas que enquadram as mesmas, serão avaliadas pelo CSGI, que poderá adotar sanções administrativas e/ou legais.

4 - Responsabilidade

Colaboradores e prestadores de serviços diretamente contratados pela empresa devem comprometer-se a agir de acordo com as políticas de Segurança da Informação.

5 – Estrutura Normativa

A estrutura normativa da Segurança da Informação da empresa é composta por um conjunto de documentos com três níveis hierárquicos:

Política de Segurança da Informação (PSI): constituída neste documento, define a estrutura, diretrizes e os papéis referentes a segurança da informação;

Normas e Planos de Segurança da Informação (Normas): estabelecem regras, definidas de acordo com as diretrizes da PSI, a serem seguidas nas diversas situações em que a informação é tratada;

Procedimentos de Segurança da Informação: instrumentam as regras dispostas nas Normas, permitindo a direta aplicação nas atividades.

5.1 – Divulgação e Acesso

A Presente Política de Privacidade deve ser divulgada ao público interno e externo, protegida contra alterações, devendo ser disponibilizada no portal interno da Creditá S.A (intranet) e na página da Creditá S.A na internet.

5.2 Aprovação e Revisão

Os documentos desta estrutura devem revisados e aprovados nos seguintes critérios:

Tipo de Doc.	Responsável	Nível de Aprovação	Periodicidade
Política	Responsável PSI	Comitê Gestor	Anual
Normas	Responsável PSI, Diretores e Gerentes	Comitê Gestor	Semestral
Procedimentos	Diretores, Gerentes e Coordenadores	Responsável PSI	Semestral

Aprovado pela diretoria em 10 de julho de 2023.